DII.31.Draft.HPSOL.AG-1

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Version 3.1 DRAFT

System Administrator's Guide (HP-UX 10.20 and Solaris 2.5.1)

April 7, 1997

Prepared for:

Defense Information Systems Agency

Prepared by:

Inter-National Research Institute (INRI)
12200 Sunrise Valley Drive, Suite 300
Reston, Virginia 20191

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

Table of Contents (continued)

List of Tables

List of Figures

This page intentionally left blank.

Preface

The following conventions have been used in this document:

[HELVETICA FONT]	Used to indicate keys to be pressed. For example, press [RETURN].
`Courier Font`	Used to indicate entries to be typed at the keyboard, operating system commands, titles of windows and dialog boxes, file and directory names, and screen text. For example, execute the following command: `tar xvf /dev/rmt/3mn`
"Quotation Marks"	Used to indicate prompts and messages that appear on the screen.
Italics	Used for emphasis.

This page intentionally left blank.

1. Introduction

This document describes general information about the Defense Information Infrastructure (DII) Common Operating Environment (COE) and the system administration utilities of the DII COE kernel.

This guide is divided into eight sections and three appendices:

Section/Appendix	Page
Introduction Provides a high-level overview of the DII COE and provides a list of additional sources of information.	3
DII COE Environment Lists hardware components and kernel components.	7
Operating Guidelines Explains startup and shutdown of the software and the hardware.	9
DII COE Kernel and Segment Installation Overview Provides instructions for performing local, remote, and network installations of the DII COE kernel and software segments.	11
Common Desktop Environment Provides information about using the Common Desktop Environment (CDE) to provide a standard environment for managing applications and functions.	13
System Administration Utilities Describes DII COE maintenance and management functions available to a system administrator.	21
Security Administration Command Line Utilities Describes how to change the security level of a workstation and enable or disable auditing.	71
Error Recovery Guidelines Describes potential problems, errors, and solutions.	75
Communications Provides information about networks, physical interfaces to the system, communications and broadcast configuration, and troubleshooting.	79
Multiple Monitor and Keyboard Configurations Shows recommended single-eye and dual-eye configuration schemes.	89
Database Size Limits Lists database limits for various DII COE files.	91

1.1 The DII COE Kernel

The DII COE kernel consists of the DII COE software required on every workstation. The kernel provides the commercial software of X Windows, Motif, and UNIX, as well as the DII COE System Administration, Security Administration, and runtime environment software. Figure 1 shows a graphical representation of the DII COE kernel and the segment installation process.

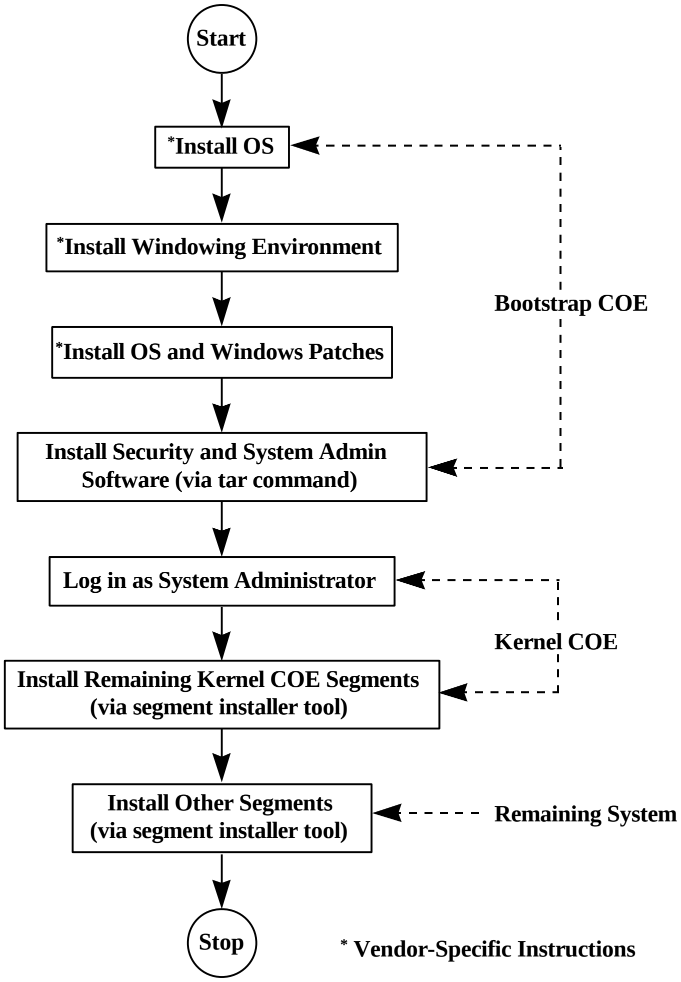

Start
*Install OS
*Install Windowing Environment
*Install OS and Windows Patches
Install Security and System Admin Software (via tar command)
Bootstrap COE
Log in as System Administrator
Install Remaining Kernel COE Segments (via segment installer tool)
Kernel COE
Install Other Segments (via segment installer tool)
Remaining System
Stop
* Vendor-Specific Instructions

Figure 1. DII COE Kernel and Segment Installation

Refer to the *DII COE Kernel Installation Guide (HP-UX 10.20)* and the *DII COE Kernel Installation Guide (Solaris 2.5.1)* for more information about installing the DII COE kernel and segments.

1.2 Additional Sources of Information

Reference the following documents for more information about the DII COE and about CDE:

C *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification* Version 2.0, DII COE I&RTS:Rev 2.0, Inter-National Research Institute, October 23, 1995

C *Defense Information Infrastructure (DII) Common Operating Environment (COE) Version 3.0.1.0 Kernel Installation Guide (HP-UX 10.20)*, DII.3010.HP1020.IG-1, Inter-National Research Institute, April 14, 1997

C *Defense Information Infrastructure (DII) Common Operating Environment (COE)* Version 3.0.0.3 *Kernel Installation Guide (Solaris 2.5.1)*, DII.3003.Final.Sol251.IG-2, Inter-National Research Institute, April 7, 1997

C *Triteal Enterprise Desktop 4.0 User's Guide*, Triteal Corporation, 1995.

This page intentionally left blank.

2. DII COE Environment

This section describes DII COE hardware components and DII COE kernel components.

Supported UNIX host computers for the current DII COE are:

C HP

C Sun SPARC.

2.1 Hardware Components

The software may reside on a single disk or across multiple disks.

2.1.1 HP Hardware

C HP 9000/7xx, with at least 64 megabytes (MB) of random access memory (RAM)

C Hard disk drive [at least 1.2 gigabytes (GB) or larger].

2.1.2 Sun SPARC Hardware

C Sun SPARC with at least 64MB of RAM

C Hard disk drive (at least 1.2GB or larger).

2.2 Kernel Components

The DII COE kernel is a suite of applications layered on top of the HP-UX or Solaris operating system. The DII COE kernel media contains software relating to several areas:

C Operating system

C System and Security Administration software

C X Windows system software

C Motif system software

C CDE

C Distributed Computing Environment (DCE).

This page intentionally left blank.

3. Operating Guidelines

This section provides operating guidelines for powering up and powering down the system.

3.1 Power Down

> **NOTE**: Never power down the system without first executing a shutdown, as described in the steps below. Doing so could cause irreparable damage.

STEP 1: **Log in**. Log in with a sysadmin account and password at the prompts.

STEP 2: **Shut down the machine**. Select the `Shutdown` option from the `Hardware` pull-down menu and respond to the appropriate prompts.

STEP 3: **Wait until the system is fully down**.

STEP 4: **Turn off the peripherals**. Turn off the peripherals, including the monitor.

STEP 5: **Turn off the computer**.

3.2 Power Up

STEP 1: **Turn on the Uninterruptable Power Supply (UPS)**. Turn on the UPS if necessary.

STEP 2: **Turn on the peripherals**. Turn on the peripherals, including the monitor.

STEP 3: **Turn on the computer**.

STEP 4: **Log in**. Log in with your assigned account and password at the prompts.

This page intentionally left blank.

4. DII COE Kernel and Segment Installation Overview

This section provides an overview of installation procedures for the DII COE kernel tape and one or more application segment tapes (e.g., Netscape).

> **NOTE**: Applications are designed to run with specific operating systems. Before installing any operating system or any segment, make sure the tape you are loading is the correct one. This can be verified by checking the label on the tape.
>
> **NOTE**: The DII COE is installed using an automated installation procedure that removes previously installed software and overwrites existing data files. This type of installation is called a *destructive installation*. Therefore, it is advised that you back up any data you want to save before beginning any installation procedure.

4.1 Installing the Operating System and Kernel

Reference the *DII COE Kernel Installation Guide (Solaris 2.5.1)* and the *DII COE Kernel Installation Guide (HP-UX 10.20)* for details on installing the operating system and kernel for the respective system.

4.2 Installing Segments

Installation of the DII COE and DII COE segments varies depending on the hardware architecture, the processor, and the type or number of segments being loaded.

Segments may be loaded or installed from tape drive or from hard disk. The source can be local, remote, or network:

C Local—from a tape drive physically attached to the machine

C Remote—from a tape drive physically attached to another machine

C Network—from a segment installation server attached to the local area network (LAN).

4.2.1 Local Installation

To install DII COE segments locally, use the segment tapes and a tape drive attached to the machine being installed. The tape drive and the distribution medium must be compatible. For example, a 4mm DAT drive cannot be used to load or install an application delivered on a cartridge tape. Installing from a local source is convenient because it does not rely on a network to reach another machine. Refer to Section 6.3.1, *Segment Installer Option*, for more information about installing segments.

4.2.2 Remote Installation

To install DII COE segments from a remote source, the machine being loaded must have network capability. In addition, you need to know the remote machine's system name or IP address. A remote source is used when a local tape drive is unavailable or when the tape drive on the machine being installed is incompatible with the tapes. For example, an HP segment can be loaded or installed from an HP workstation or from a Sun SPARCstation. Refer to Section 6.3.1, *Segment Installer Option*, for more information about installing segments.

4.2.3 Network Installation

To install DII COE segments from a network source, the segments must first be loaded onto one or more segment servers (the hard disk of one or more network machines). Loading a segment is different than installing a segment. Loading a segment on a machine stores the segment on the machine, but does not enable the segment to run. Instead, segments stored on a segment installation server are available for installation without the installation medium because they are located on a server. Segments can, then, be installed individually on each machine on the network. However, network installations require the system to be configured with networking capabilities. Refer to Section 6.3.2, *Segment Installation Server Option*, for more information about loading segments on a segment installation server.

NOTE: Loading segments on multiple machines is highly recommended because it ensures easy access to the software and does not require the user to locate segment installation tapes.

5. Common Desktop Environment

The DII COE kernel is a suite of applications layered on top of the HP-UX or Solaris Operating System. The Common Desktop Environment (CDE) is one of several software programs that comprise the kernel. CDE provides a standard environment for managing applications and functions within one or more workspaces. To help organize your desktop, you can place special applications in a particular workspace and name that workspace accordingly.

The CDE has a horizontal window at the bottom of the display called a Front Panel, which is a desktop window that exists in all workspaces. The CDE remains open as different workspaces are opened. Figure 1 shows a CDE Front Panel. The panel below includes the following icons: Clock, Calendar, File Manager, Text Editor, Mailer, Workspace Switch, lock, Graphical Workspace Manager (GWM), EXIT, Default Printer, Style Manager, Application Manager, Help Manager, and Trash Can. These icons are controls and indicators for completing tasks. The controls and indicators shown in Figure 2 are described in greater detail in the following subsections.

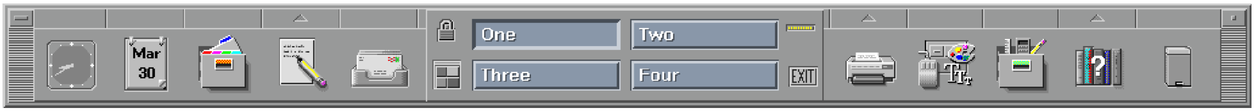


Figure 2. CDE Front Panel

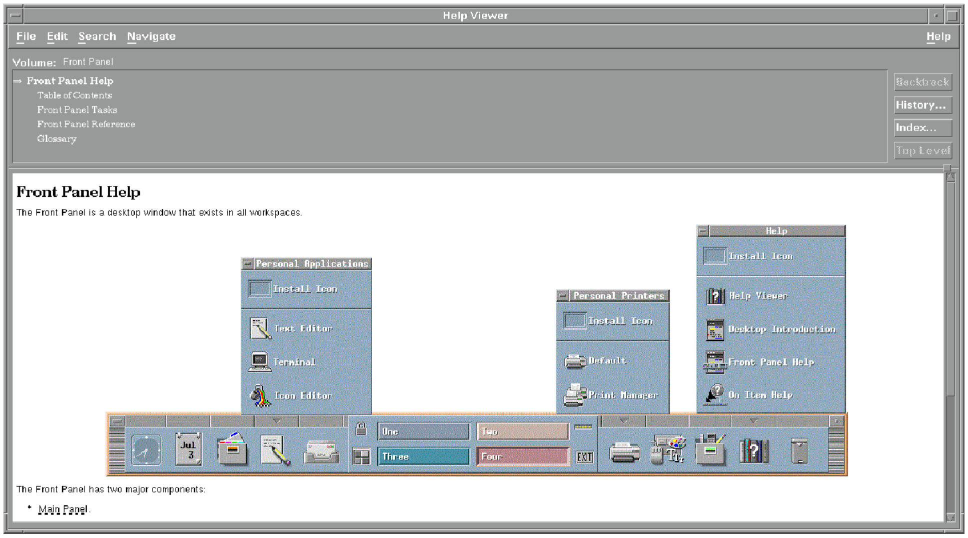
5.1 Subpanels

The default Front Panel contains subpanels. Controls with subpanels have a button with an upward arrow above them. This button is used to display or close the subpanel. For example, the Text Editor—Personal Applications, Personal Printers, and Help Manager controls have subpanels (Figure 3). Subpanels contain an `Install Icon` control, which allows the user or system administrator to customize the Front Panel, an icon that will start the application, and other controls. Dropping a file, folder, or action icon on the `Install Icon` control installs the file, folder, or action item in that subpanel.

To open a subpanel, click the arrow button above the control. To close a subpanel, click the down arrow that appears at the bottom of the subpanel.

NOTE: If you have not moved a subpanel from its initial position, it closes automatically when you choose a control.

Initially, the Text Editor—Personal Applications, Personal Printers, and Help Manager controls have subpanels. In addition, you can add subpanels to other controls. The CDE can be customized: Your front panel may contain additional subpanels, and the subpanels may contain additional or different controls. In other words, you can add controls to subpanels, interchange Front and subpanel controls, add subpanels, add or delete workspaces, or rename workspaces.



Front Panel Help

The Front Panel is a desktop window that exists in all workspaces.

The Front Panel has two major components:

- Main Panel.

Figure 3. CDE Subpanels

5.1.1 Adding and Removing Subpanels

Follow the steps below to add or remove a subpanel.

STEP 1: **Indicate which subpanel should be added or removed**. Point to the control in the front panel whose subpanel you want to add or remove.

STEP 2: **Add or remove the subpanel**. Choose `Add Subpanel` or `Delete Subpanel` from the control's pop-up menu (see subsection 5.3, *Pop-up Menus*, for more information about pop-up menus).

5.1.2 Moving a Subpanel

Follow the steps below to move a subpanel.

STEP 1: **Indicate which subpanel should be moved**. Point to the subpanel's window frame.

STEP 2: **Move the subpanel**. Hold down the left mouse button as you drag the subpanel to its new location.

5.2 Controls and Indicators

The CDE contains controls and indicators. A control, when selected, allows the user to access applications and utilities. The Calendar, File Manager, Mailer, Workspace Switch, Lock, Graphical Workspace Manager (GWM), Exit, Printer, Style Manager, Application Manager, Help Manager, and Trash Can are examples of controls. An indicator does not have a specific action when selected—it simply provides information. The Clock and the Busy Light are two examples of indicators.

The default indicators and controls that comprise the CDE are described in the following subsections as they appear from left to right on the CDE front panel. Since it can be customized, your Front Panel may contain additional or different controls. Reference the *Triteal Enterprise Desktop 4.0 User's Guide* for additional information on the CDE.

5.2.1 Clock

The Clock is an indicator that displays the current time, which is maintained by the operating system.

5.2.2 Calendar

The Calendar is a control that displays the system date. Click on the Calendar to start the Calendar application. The Calendar application enables scheduling of appointments and creation of To Do lists. Day, week, month, and year calendar views are available. Appointments can be scheduled, deleted, and listed.

5.2.3 File Manager

The File Manager control opens a view of your home folder or of a selected folder. This application is used to manage the files and directories of a system, as well as to create, edit, rename, and delete files and folders. Click on the File Manager control to open a view of your home folder, or drop a file on the File Manager control to open a view of the dropped folder.

5.2.4 Text Editor—Personal Applications

The Text Editor—Personal Applications control is used to edit text. Click on the Text Editor control to start the desktop Text Editor application. Dropping a file on the Text Editor control opens the file in a new Text Editor window.

This control position is reserved for a personal application of your choice. To place an application other than the Text Editor in this control position, install the new application icon in the Personal Applications subpanel. Applications are installed from the Application Manager (see Section 5.2.13, *Application Manager*) by dragging the icon from the Application Manager window to the Install Icon control. Once the application is installed in the Personal Applications subpanel, you can use the control’s pop-up menu to place that control in the Front Panel.

NOTE: These icons may not function based on profile selection.

Using this same installation process, you can store frequently used applications in the Personal Applications subpanel, such as the Terminal control, and the Icon Editor control. These two controls are discussed in the following subsections.

5.2.4.1 Terminal

The Terminal control is used to open a terminal emulator window. Click on the Terminal control to open the window.

NOTE: For security reasons, this option has been removed from the CDE Front Panel for all users except root. Root users can access the Terminal control from the Text Editor**—**Personal Applications control subpanel.

If you are logged in with a System Administration account and want to access a terminal emulator window, follow the steps below:

STEP 1: Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.

STEP 2: Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS`folder.

STEP 3: Double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window. This window contains both a `Dtterm` icon and an `Xterm` icon.

STEP 4: Double-click on either the `Dtterm` icon or the `Xterm` icon to open the window.

5.2.4.2 Icon Editor

The Icon Editor control is used to create new icons (bitmap and pixmap files) or edit existing icons. Click on the Icon Editor control to open the Icon Editor application.

5.2.5 Mailer

The Mailer control is used to create, send, and receive electronic messages and attachment files. Click on the Mailer control to start the Mailer application. To mail one or more files, select the file(s) in File Manager, drag the file(s) from File Manager and drop them on the Mailer control, type the subject and destination address(es) into the `New Message` dialog box, and click on the `Send` button.

The Mailer control includes an indicator, which indicates the arrival of new mail. Dropping a file on the Mailer control opens the file’s contents in the Mailer’s New Message window.

5.2.6 Workspace Switch

The Workspace Switch allows you to change workspaces. To help organize your desktop, you can place special applications in a particular workspace and name that workspace accordingly. Each workspace, therefore, contains only those applications and functions you want to group together. The Workspace Switch is located in the center of the CDE Front panel. It contains buttons with the words "`One`", "`Two`", "`Three`", and "`Four`", which are controls used to select one of four workspaces. The button for the current workspace is “pushed in” (i.e., inset from the other three). To change the name of the current workspace, click its button and edit the name in the button.

5.2.7 Lock Control

The Lock icon locks the display and keyboard, thereby preventing unauthorized input. No input from your keyboard or mouse will be allowed until you unlock the display with your password. Click on the Lock control to lock the display.

5.2.8 GWM Control

The GWM control is used to start the Graphical Workspace Manager (GWM), which provides a visual representation of the application windows available in all of the workspaces. The GWM is used to control the size, placement, and operation of windows within multiple workspaces, as well as maintain a depiction of the windows as the user creates, moves, and otherwise manipulates them. Click on the GWM control to start the GWM application.

5.2.9 Busy Light Indicator

The Busy Light indicator blinks to indicate that the system is running an action.

5.2.10 EXIT Control

The EXIT control is used to log out of the desktop and end the desktop session. Click on the EXIT control to end the current session.

5.2.11 Personal Printers

The Personal Printers control displays the status of the default printer and allows cancellation of print jobs on that printer. Click on the Printer control to open the Printer Jobs dialog box, which shows the status of print jobs on the default printer. Drag a file from the Application Manager of the File Manager and then drop them onto the Printer control to print them on the default printer.

The Personal Printers subpanel contains the following applications: Install Icon, Default Printer, and Print Manager. Install Icon is used to install an icon dragged from File Manager or Application Manager onto the subpanel. Print Manager is used to print a file on the default printer.

5.2.12 Style Manager

The Style Manager is used to customize the appearance and behavior of your desktop session. Specifically, the Style Manager control allows customization of the backdrop, keyboard, screen, fonts, colors, mouse, startup, beep, and window. Click on the Style Manager control to start the Style Manager application. If the application is already running, its window is raised to the top of the window stack.

5.2.13 Application Manager

The Application Manager is a container for the applications registered on your system. Click on the Application Manager control to open an `Application Manager` window. This window contains folders of application groups, such as tools and applications. These folders contain icons that, when selected, start applications.

5.2.14 Help Manager

The Help Manager control lists information about CDE topics. Click on the Help Manager control to open a `Help View` window displaying the top level of help information. The help available on your system is organized hierarchically. The top level lists all the help "families" on your system. When you click on a family to open it, you will see a list of all the help "volumes" in that family. The Index feature in the `Help View` window is used to search for topics.

The Help Manager subpanel contains the following applications: Desktop Introduction, which provides an introduction to the desktop; Front Panel Help, which provides an introduction to the front panel of the CDE; and On-Item Help, which provides information on a selected control.

5.2.15 Trash Can

The Trash Can stores files for deletion. Click on the Trash Can control to open the `Trash Can` window. Dropping a file or folder on the Trash Can control moves the file or folder to the Trash Can. The Trash Can is emptied by opening the Trash Can, selecting files to be deleted, choosing `Shred` from the `File` menu or from the `Trash Can` pop-up menu, and then clicking `OK` in the confirmation window.

5.3 Pop-up Menus

CDE Front Panel controls include pop-up menus. The contents of a control's pop-up menu depends on the behavior of the control and its location. To display a Front Panel pop-up menu, point to the control and press the right mouse button.

5.3.1 Pop-up Menus for Front Panel Controls

If the control starts an application, the first entry in the menu is a command that starts the application. Choosing the menu option has the same effect as clicking on the control. If the Front Panel control does not have a subpanel, clicking on the control with the right mouse button will display the following pop-up menu options: `[Name of the control]`, `Add Subpanel`, and `Help`.

`[Name of the control]`
Starts the application (if the control starts an application).

`Add Subpanel`
Adds a subpanel to the control.

`Help`
Displays on-line help for the control.

5.3.2 Pop-up Menus for Front Panel Controls with Subpanels

If the Front Panel control has a subpanel, clicking on the control with the right mouse button will display the following pop- up menu: `[Name of the control]`, `Remove Subpanel`, and `Help`.

`[Name of the control]`
Starts the application (if the control starts an application).

`Remove Subpanel`
Removes the subpanel and its contents.

`Help`
Displays on-line help for the control.

5.3.3 Pop-up Menu for the Switch Area

The switch area is the portion of the workspace switch not occupied by other controls or workspace buttons. The pop-up menu contains the following options: `Add Workspace` and `Help`.

`Add Workspace`
Adds a workspace.

`Help`
Displays help for the workspace switch.

5.3.4 Pop-up Menu for Workspace Buttons

Workspace buttons are used to change workspaces. Each button has its own menu, which contains the following options: `Add Workspace`, `Delete`, `Rename`, and `Help`.

`Add Workspace`
Adds a workspace.

`Delete`
Deletes the workspace.

`Rename`
Turns the button label into a text field for editing the name.

`Help`
Displays help for the workspace switch buttons.

5.3.5 Pop-up Menu for Subpanel Controls

The pop-up menu for subpanel controls includes a command for making a particular control the current Front Panel control. The pop-up menu contains the following options: `Copy to Main Panel`, `Remove`, and `Help`.

`Copy to Main Panel`
Duplicates the control in the Front Panel, replacing the current Front Panel control.

`Remove`
Removes the control from the subpanel.

`Help`
Displays on-line help for the control.

6. System Administration Utilities

This section describes the DII COE System Administration application, which provides options for DII COE maintenance and management. To access utilities, log in with a system administration user account.

Options are grouped according to their functionality and are located on pull-down menus or as icons within the application manager. Some options may have a cascading menu. Availability of specific menu options depends on two criteria:

- Hardware type (e.g., HP or SPARC)

- Access assigned to the user account profile.

The System Administration application has the following pull-down menus: `SA System`, `Hardware`, `Software`, and `Network`. In addition, one system administration task may be performed from the command line: removing global data. These system administration utilities are described in the following sections.

6.1 SA System Menu

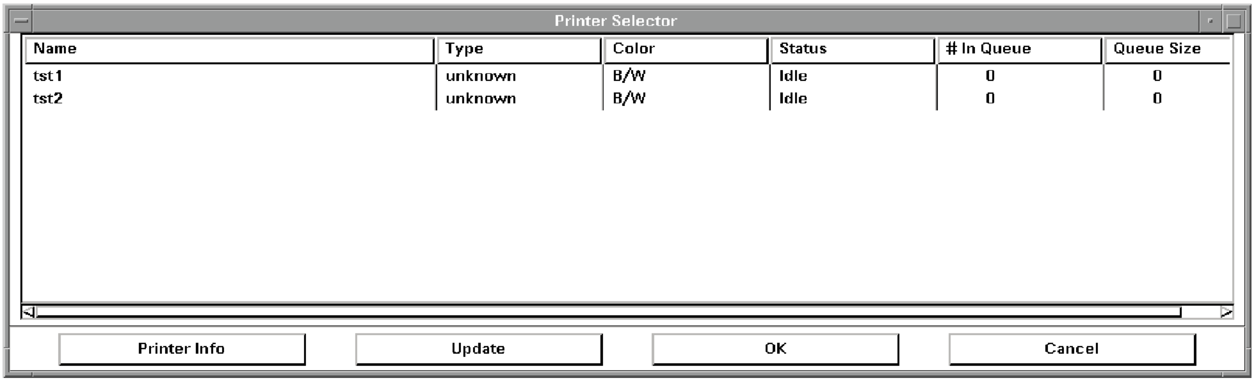
The `SA System` menu contains the following options: `Printer` and `Close All`. These options are described in the subsections below.

6.1.1 Printer Option

The `Printer` option is used to select a default printer and to view print jobs stored in the local queue. The `Printer` option has a cascading menu that contains two options: `Printer Select` and `Print Jobs`.

6.1.1.1 Printer Select Option

The `Printer Select` option is used to select a default printer. After selecting the `Printer Select` option, the `Printer Selector` window appears (Figure 4). The window shows all printer selections. The default printer will be highlighted. To change the default printer, click on a different printer to highlight it and click on the `OK` button.



Name	Type	Color	Status	# In Queue	Queue Size
tst1	unknown	B/W	Idle	0	0
tst2	unknown	B/W	Idle	0	0

Figure 4. Printer Selector Window

Printer Selector Window Fields

The `Printer Selector` window has the following fields: `Name`, `Type`, `Color`, `Status`, `# In Queue`, and `Queue Size`. These fields are described below.

`Name`
Lists printer names. The printer selections listed in this field are selected using the Admintool for Solaris and SAM (system administration manager tool) for HP. Admintool and SAM are located in the `Application Manager - SA_Default` window. To access this window, double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window, double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS`folder, and double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window.

NOTE: Refer to vendor documentation for information on using SAM and Admintool to add printers to the `Printer Selector` window.

`Type`
Shows the printer type.

`Color`
Shows the viewing option (color or black and white).

`Status`
Shows the status of the printer. Sample statuses are `Idle` (printer is currently idle), `Busy` (printer is currently processing jobs), `Error` (printer has detected an error), and `Unknown` (unable to determine the printer status).

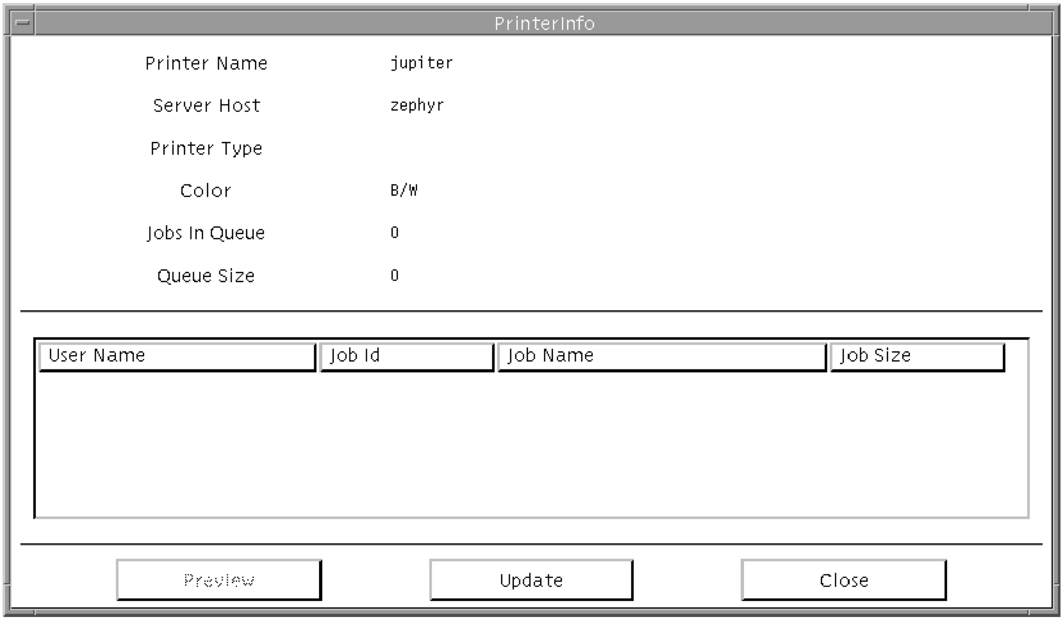
`# In Queue`
Shows the number of print jobs in the print queue.

`Queue Size`
Shows the total size of all jobs in the queue.

Printer Selector Window Buttons

The `Printer Selector` window has the following buttons: `Printer Info`, `Update`, `OK`, and `Cancel`. These buttons are described below.

`Printer Info`
Used to show information about each printer selection listed in the `Printer Selector` window. To show information about print jobs queued to a specific printer listed in the `Printer Selector` window, click on a printer to highlight it and click on the `Printer Info` button. The `PrinterInfo` window appears (Figure 5). This window shows the printer name, server host, printer type, color (e.g., color or black and white), number of jobs in the queue, and queue size for the selected printer. It also shows the user name of the person who sent each print job to the selected printer, each job ID, each job name, and each job size.



Printer Name jupiter
Server Host zephyr
Printer Type
Color B/W
Jobs In Queue 0
Queue Size 0

User Name	Job Id	Job Name	Job Size

Figure 5. PrinterInfo Window

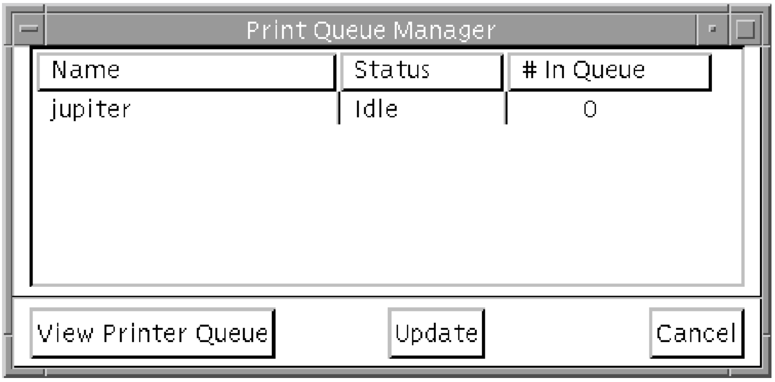
Update
Used to update entries on the Printer Selector window.

OK
Used to save any changes made to the default printer.

Cancel
Used to close the Printer Selector window.

6.1.1.2 Print Jobs Option

The Print Jobs option is used to allow the user to view the print jobs stored in the local queue. After selecting the Print Jobs option, the Print Queue Manager window appears (Figure 6).



Name	Status	# In Queue
jupiter	Idle	0

Figure 6. Print Queue Manager Window

Print Queue Manager Fields

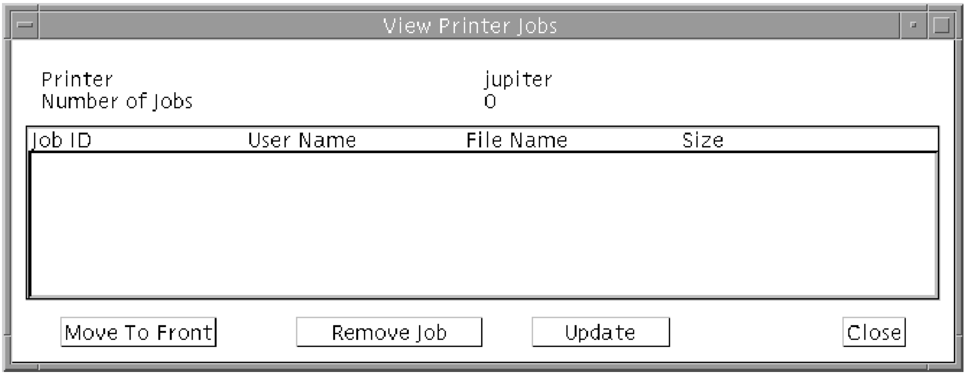
The Print Queue Manager window has the following fields: Name, Status, and # In Queue. These fields are described below.

Name
Shows the printers supported on the system.

Status
Shows the status of the printer (e.g., Idle, Busy, Error, Unknown).

# In Queue
Shows the number of print jobs in the print queue.

To show the print jobs for a specific printer listed in the Print Queue Manager window, click on a printer in the list to highlight it and click on the View Printer Queue button. The View Printer Queue button is used to provide information about print jobs in the local queue. The View Printer Jobs window appears (Figure 7).



Printer jupiter
Number of Jobs 0

Job ID	User Name	File Name	Size

Figure 7. View Printer Jobs Window

View Printer Jobs Window Fields

The `View Printer Jobs` window has the following fields: `Job ID`, `User Name`, `File Name`, and `Size`. These fields are described below.

`Job ID`
Shows the ID number automatically assigned by the system.

`User Name`
Shows the name of the user who sent the job to the printer.

`File Name`
Shows the name of the file sent to the printer.

`Size`
Shows the size of the print file in bytes.

View Printer Jobs Window Buttons

The `View Printer Jobs` window has the following buttons: `Move To Front`, `Remove Job`, `Update`, and `Close`. These buttons are described below.

`Move To Front`
Used to change the priority of a selected print job in the printer queue. To move a print job to the front of the queue, click on the print job in the `View Printer Jobs` window to highlight it and click on the `Move To Front` button.

`Remove Job`
Used to remove a print job from the printer queue. To remove a print job, click on the print job in the `View Printer Jobs` window to highlight it and click on the `Remove Job` button.

`Update`
Used to update entries in the `View Printer Jobs` window.

`Close`
Used to close the `View Printer Jobs` window and return to the `Print Queue Manager` window.

6.1.2 Close All Option

The `Close All` option is used to close all the windows launched from the menu bar or from the `DII_APPS` folder. To access the `DII_APPS` folder, double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window. The `DII_APPS` folder is located in this window.

> **NOTE**: The `Close All` option does not close windows opened from the CDE front panel. Refer to Section 5, *Common Desktop Environment*, for more information about CDE.

6.2 Hardware Menu

The `Hardware` menu contains the following options: `Shutdown System`, `Reboot System`, and `Disk Manager`. These options are described in the following subsections.

6.2.1 Shutdown System Option

The `Shutdown System` option is used to shut down the system safely before powering down the machine.

> **NOTE**: Never power down the system without first executing a shutdown, as described in the steps below. Doing so could cause irreparable damage.

Follow the steps below to shutdown the system.

STEP 1: **Select the `Shutdown System` option**. The `Shutdown` dialog box appears with the following message: `Do you want to shutdown the computer?`

STEP 2: **Shut down the system**. Click on the `OK` button to continue the shutdown process.

STEP 3: **Turn off the system**. Turn off the machine when the system is completely down. System messages appear that indicate the system is ready to power down.

6.2.2 Reboot System Option

The `Reboot System` option is used to reboot the system. Follow the steps below to reboot the system.

STEP 1: **Select the `Reboot System` option**. The `Reboot` dialog box appears with the following message: `Do you want to shutdown and reboot the computer?`

STEP 2: **Reboot the system**. Click on the `OK` button to reboot the machine. When the reboot is complete, the DII COE Login window appears.

6.2.3 Disk Manager Option

The `Disk Manager` option provides the following file system management functionality:

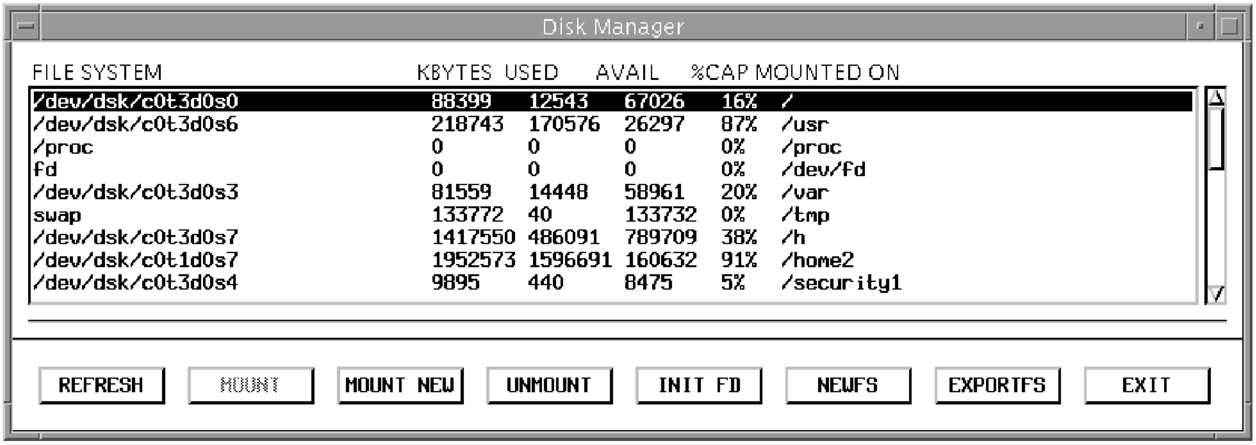
C Mounts file system partitions

C Formats hard drives

C Displays hard disk space availability

C Initializes floppy diskettes.

After selecting the `Disk Manager` option, the `Disk Manager` window appears (Figure 8).



```
FILE SYSTEM                  KBYTES  USED    AVAIL   %CAP MOUNTED ON
/dev/dsk/c0t3d0s0            88399   12543   67026   16%  /
/dev/dsk/c0t3d0s6            218743  170576  26297   87%  /usr
/proc                        0       0       0       0%   /proc
fd                           0       0       0       0%   /dev/fd
/dev/dsk/c0t3d0s3            81559   14448   58961   20%  /var
swap                         133772  40      133732  0%   /tmp
/dev/dsk/c0t3d0s7            1417550 486091  789709  38%  /h
/dev/dsk/c0t1d0s7            1952573 1596691 160632  91%  /home2
/dev/dsk/c0t3d0s4            9895    440     8475    5%   /security1
```

Figure 8. Disk Manager Window

A mounted file system can be accessed for read and write operations. Mounted file systems are highlighted in yellow.

Disk Manager Window Buttons

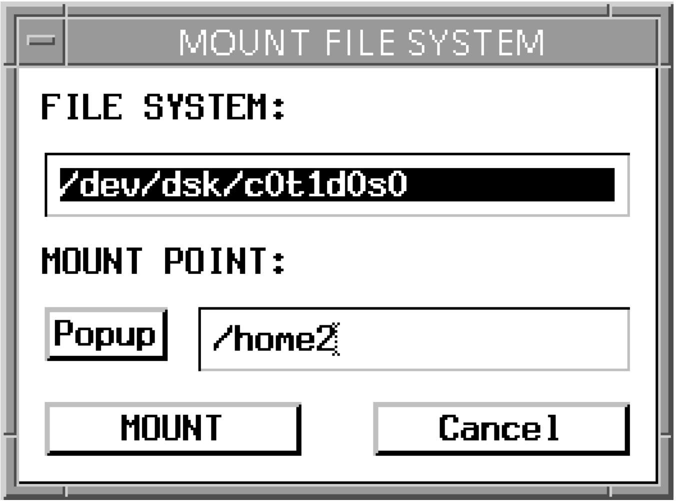
The `Disk Manager` window has the following buttons: `REFRESH`, `MOUNT`, `MOUNT NEW`, `UNMOUNT`, `INIT FD`, `NEWFS`, `EXPORTFS`, and `EXIT`. These buttons are described below.

`REFRESH`
Used to update file system entries in the `Disk Manager` window.

`MOUNT`
Used to attach an existing file system listed in the `Disk Manager` window to a directory, thereby making the files available to the user. Follow the steps below to mount a file system.

STEP 1: **Select a file system to be mounted**. Click on a file system in the `Disk Manager` window to highlight it.

STEP 2: **Click on the `MOUNT` button**. The `MOUNT FILE SYSTEM` window appears (Figure 9).



MOUNT FILE SYSTEM

FILE SYSTEM:

/dev/dsk/c0t1d0s0

MOUNT POINT:

/home2

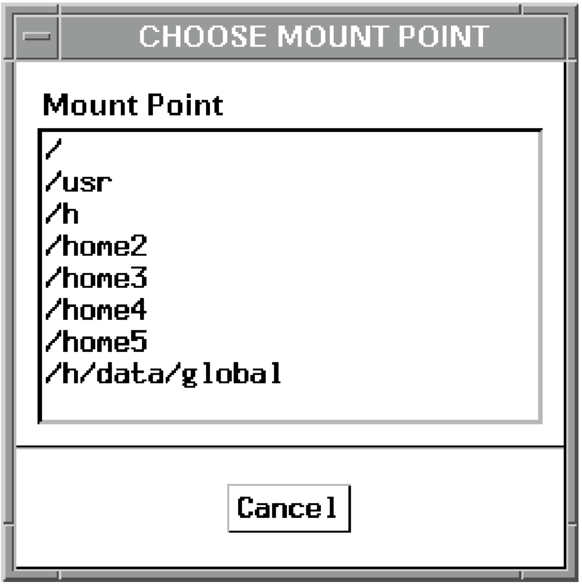
Figure 9. MOUNT FILE SYSTEM Window

STEP 3: **Select an unused location as a mount point for the file system**. Enter a mount point in the `MOUNT POINT` field. Enter a mount point in one of two ways:

(a) Type the location, if known, in the `MOUNT POINT` field.

OR

(b) Toggle on the `Popup` checkbox to the left of the `MOUNT POINT` field to open the `CHOOSE MOUNT POINT` window (Figure 10). Click on a mount point from the scroll list to select it. The `MOUNT FILE SYSTEM` window reappears with the new mount point in the `FILE SYSTEM` field.



CHOOSE MOUNT POINT

Mount Point

/
/usr
/h
/home2
/home3
/home4
/home5
/h/data/global

Figure 10. CHOOSE MOUNT POINT Window

STEP 4: **Mount the file system**. Click on the MOUNT button in the MOUNT FILE SYSTEM window.

STEP 5: **Determine if the file system should be mounted each time the system is rebooted**. Select YES or NO at the following prompt: Do you want to permanently mount the file system?If you select NO, then that data will not be available to the user the next time the machine is rebooted.

MOUNT NEW

Used to identify a new file system and attach it to a directory, thereby making that directory structure available to the user. Once mounted, the file system is listed in the Disk Manager window. Follow the steps below to identify a new file system:

STEP 1: **Click on the MOUNT NEW button**. The MOUNT FILE SYSTEM window appears (Figure 9).

STEP 2: **Select the new file system to be created**. Enter the new file system name in the FILE SYSTEM field.

STEP 3: **Select an unused location as a mount point for the file system**. Enter a mount point in the MOUNT POINT field to select an unused location to mount the file system. Enter a mount point in one of two ways:

(a) Type the location, if known, in the MOUNT POINT field.

OR

(b) Toggle on the Popup checkbox to the left of the MOUNT POINT field to open the CHOOSE MOUNT POINT window (Figure 10).Click on a mount point from the scroll list to select it. The MOUNT FILE SYSTEM window reappears with the new mount point in the FILE SYSTEM field.

STEP 4: **Mount the new file system**. Click on the MOUNT button in the MOUNT FILE SYSTEM window.

STEP 5: **Determine if the file system should be mounted each time the system is rebooted**. Select YES or NO at the following prompt: Do you want to permanently mount the file system?If you select NO, then that data will not be available to the user the next time the machine is rebooted.

`UNMOUNT`

Used to unattach a file system listed in the `Disk Manager` window to a directory. When a file system is unmounted, the files become unavailable to the user, yet they remain intact.

> **NOTE**: A file system that is in use cannot be unmounted.

Follow the steps below to unmount a file system.

STEP 1: **Select a file system to be unmounted**. Click on a file system in the `Disk Manager` window to highlight it.

STEP 2: **Click on the `UNMOUNT` button**.

STEP 3: **Determine if the file system should be permanently unmounted**. Select `YES` or `NO` at the following prompt: `DO YOU WANT TO PERMANENTLY UNMOUNT THE FILESYSTEM?` If you select `NO`, then that data will be available to the user the next time the machine is rebooted.

`INIT FD`

Used to format a floppy diskette. Follow the steps below to format a floppy diskette.

STEP 1: **Click on the `INIT FD` button**.

STEP 2: **Confirm that the floppy diskette should be formatted**. Click on the `CONTINUE` button in the `WARNING` window to initialize the disk, or click on the `CANCEL` button to return to the `Disk Manager` window.

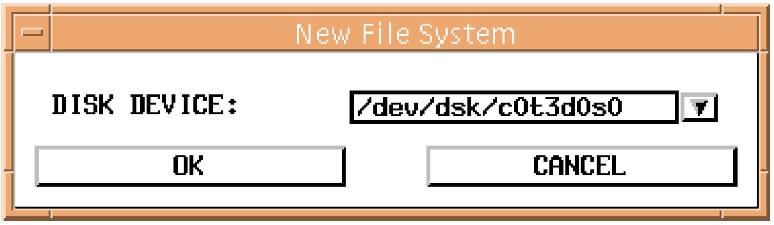
> **WARNING**: The `INIT FD` option erases the entire contents of the floppy diskette.

NEWFS

Used to reformat a selected device to create a new file system. Follow the steps below to create a new file system.

> **WARNING**: All data on the selected device will be deleted. No partitions are protected from NEWFS. Therefore, it is advised that you back up any data you want to save before beginning any NEWFS procedure.

STEP 1: **Click on the NEWFS button**. The New File System window appears (Figure 11).



DISK DEVICE: /dev/dsk/c0t3d0s0

Figure 11. New File System Window

STEP 2: **Select the disk device to be reformatted**. Select the device in one of two ways:

(a) Type the name of the disk device in the DISK DEVICE field.

OR

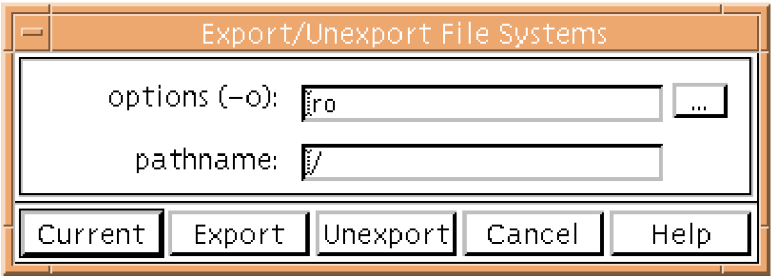
(b) Click on the arrow and then click on a disk device from the list to select it.

STEP 3: **Click on the OK button**.

STEP 4: **Confirm that the new file system should be created**. Click on the CONTINUE button in the WARNING window to format the device, or click on the CANCEL button to discard the process.

EXPORTFS

Used to export or unexport a file system in order to allow or deny file system sharing. After selecting the EXPORTFS option, the Export/Unexport File Systems window appears (Figure 12).



options (-o): ro

pathname: /

Figure 12. Export/Unexport File Systems Window

Export/Unexport File Systems Window Buttons

Current
Used to show the file systems that are currently exported (shared).

Export
Used to export (share) a selected file system permanently.

Unexport
Used to unexport (deny file system sharing to) a selected file system permanently.

Cancel
Used to close the `Export/Unexport File Systems` window.

Help
Used to show a manual page for the `EXPORTFS` option.

Follow the steps below to export a file system.

STEP 1: **Select a file system**. Click on a file system in the list in the `Disk Manager` window to highlight it and then click on the `EXPORTFS` button. The `Export/Unexport File Systems` window appears (Figure 12).

STEP 2: **Enter options**. Click on the `options` field toggle to view a list of options. Click on one or more options from the list (e.g., read only, read/write) to select them. The options then appear in the `options` field.

STEP 3: **Enter a pathname**. Enter the actual pathname of the directory you want to share in the `pathname` field.

STEP 4: **Export the file system**. Click on the `Export` button.

STEP 5: **Determine if the file system should be exported or unexported permanently**. Click on the `Yes` or the `No` button when the following prompt appears: `Do you want to permanently export the file system?` The window closes.

STEP 6: **Confirm that the file was exported**. Click on the `Current` button in the `Disk Manager` window. The shared directory should appear in the list of exported file systems.

NOTE: Refer to the EXPORTFS manual page for more information about the `EXPORTS` option. Click on the `Help` button in the `Export/Unexport File Systems` window to view the EXPORTFS manual page.

EXIT
Used to close the `Disk Manager` window and exit the `Disk Manager` option.

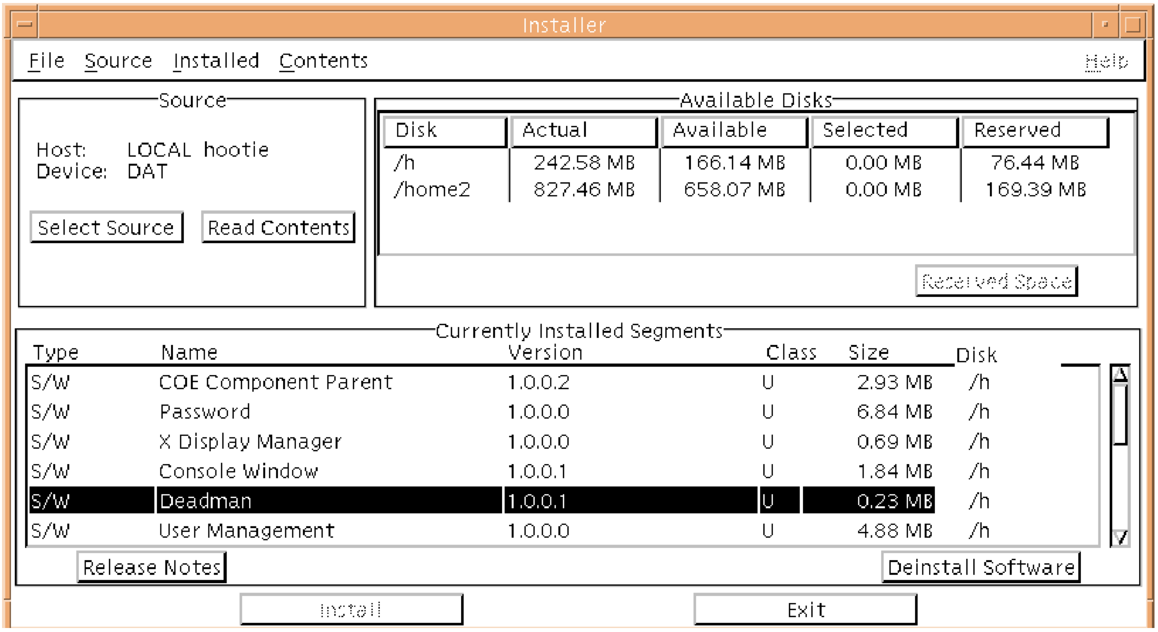
6.3 Software Menu

The `Software` menu contains two options: `Segment Installer` and `Segment Installation Server`. These options are described in the following subsections.

6.3.1 Segment Installer Option

The `Segment Installer` option is used to install segments. Select the `Segment Installer` option to open the `Installer` window (Figure 13).

> **NOTE**: Ensure that you can see the whole window by clicking on the bottom right edge of the window and dragging the trackball or mouse outward to enlarge the window.



Host: LOCAL hootie
Device: DAT

Disk	Actual	Available	Selected	Reserved
/h	242.58 MB	166.14 MB	0.00 MB	76.44 MB
/home2	827.46 MB	658.07 MB	0.00 MB	169.39 MB

Type	Name	Version	Class	Size	Disk
S/W	COE Component Parent	1.0.0.2	U	2.93 MB	/h
S/W	Password	1.0.0.0	U	6.84 MB	/h
S/W	X Display Manager	1.0.0.0	U	0.69 MB	/h
S/W	Console Window	1.0.0.1	U	1.84 MB	/h
S/W	Deadman	1.0.0.1	U	0.23 MB	/h
S/W	User Management	1.0.0.0	U	4.88 MB	/h

Figure 13. Installer Window

6.3.1.1 Installer Window Pull-down Menus

The `Installer` window has the following pull-down menus: `File`, `Source`, `Installed`, and `Contents`. These pull-down menus are described below.

`File`

The `File` pull-down menu contains the following options: `Install` and `Exit`.

`Install`
Allows the user to install selected segments. Performs the same functionality as clicking on the `Install` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Install` button.

`Exit`
Exits the user from the `Installer` window. Performs the same functionality as clicking on the `Exit` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Exit` button.

`Source`

The `Source` pull-down menu contains the following options: `Select Source` and `Read Contents`.

`Select Source`
Displays the currently selected installation media. Performs the same functionality as clicking on the `Select Source` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Select Source` button.

`Read Contents`
Allows the user to read the table of contents of the selected installation device. Performs the same functionality as clicking on the `Read Contents` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Read Contents` button.

`Installed`

The `Installed` pull-down menu contains the following options: `Release Notes`, `Deinstall Software`, and `View Installation Log`.

`Release Notes`
Displays release notes information for any selected segment. Performs the same functionality as clicking on the `Release Notes` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Release Notes` button.

`Deinstall Software`
Allows the user to deinstall segments highlighted in the `Currently Installed Segments` panel. Performs the same functionality as clicking on the `Deinstall Software` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Deinstall Software` button.

`View Installation Log`
Displays a detailed log of the installation process.

`Contents`

The `Contents` pull-down menu contains the following options: `Release Notes`, `Required Software`, and `Conflicting Software`.

`Release Notes`
Displays release notes information for any selected segment. Performs the same functionality as clicking on the `Release Notes` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Release Notes` button.

`Required Software`

Lists segments that need to be installed in order to install the segment selected in the `Select Segment To Install` panel. Performs the same functionality as clicking on the `Requires` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Requires` button.

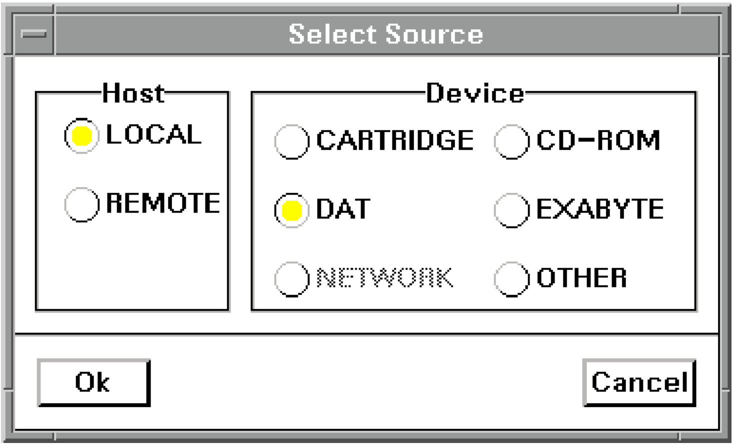
`Conflicting Software`
Lists the segments that cannot be installed with the segment selected in the `Select Segment To Install` panel. Performs the same functionality as clicking on the `Conflicts` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Conflicts` button.

6.3.1.2 Installer Window Panels

The `Installer` window has the following panels: `Source`, `Available Disks`, `Currently Installed Segments`, and `Select Software To Install`. The `Select Software To Install` panel does not appear in the `Installer` window shown in Figure 13—it only appears after the `Read Contents` button has been selected in the `Source` panel. The `Installer` window panels are described below.

`Source`
Displays the name of the host machine, the name of the installation device, and the table of contents of that installation device. The `Source` panel has two buttons: `Select Source` and `Read Contents`.

`Select Source`
Used to display the currently selected installation media. Click on the `Select Source` button to open the `Select Source` window (Figure 14). This window allows the user to select the installation source device. The device selection defaults to the DAT drive on the local machine (the `LOCAL` option in the `Host` panel and the `DAT` option in the `Device` panel).



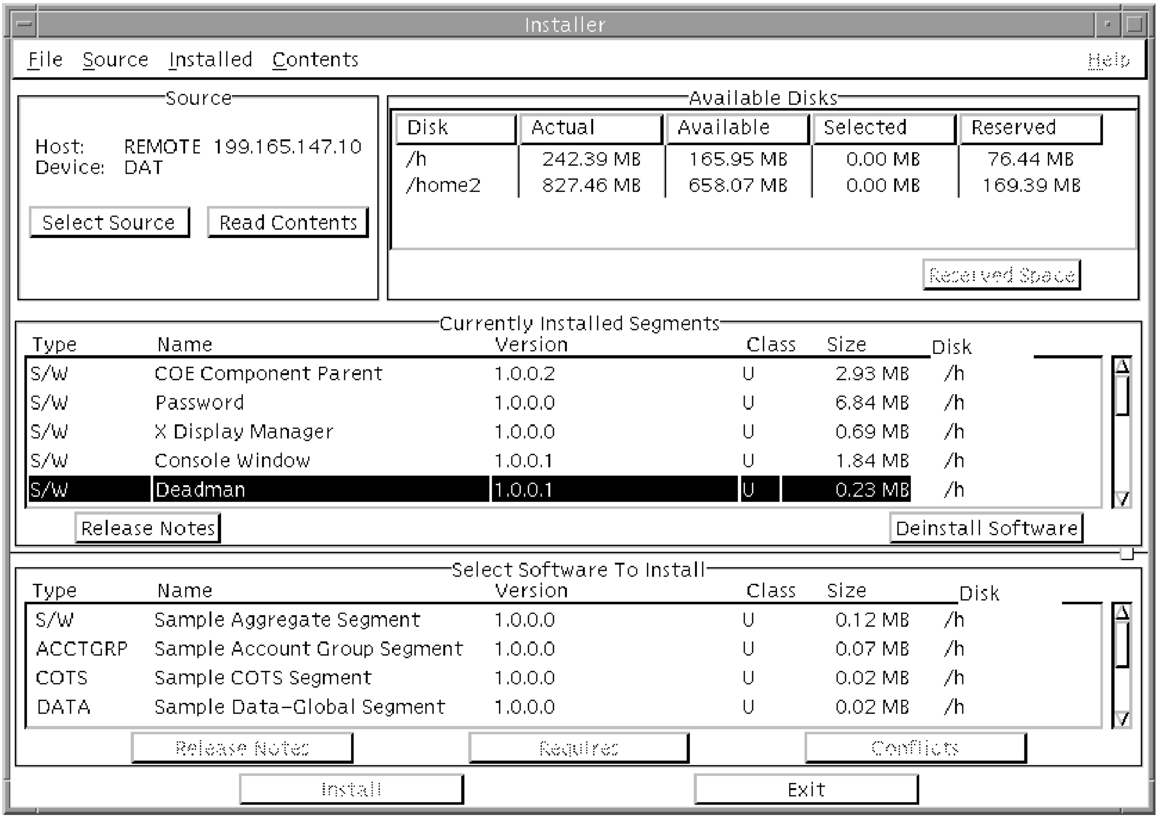
Host
● LOCAL
○ REMOTE

Device
○ CARTRIDGE ○ CD-ROM
● DAT ○ EXABYTE
○ NETWORK ○ OTHER

Figure 14. Select Source Window

`Read Contents`

Used to read the table of contents of the selected installation device. Click on a segment listed in the `Installer` window to highlight it and then click the `Read Contents` button. The media will be scanned for the segments that it contains, and then the `Installer` window will add the `Select Software To Install`panel, which lists the segments that the media contains (Figure 15). Any number of segments may be selected in this panel for installation. See Section 6.3.1.3, *Installing Segments*, for additional information about the segment installation process.



Host: REMOTE 199.165.147.10
Device: DAT

Disk	Actual	Available	Selected	Reserved
/h	242.39 MB	165.95 MB	0.00 MB	76.44 MB
/home2	827.46 MB	658.07 MB	0.00 MB	169.39 MB

Currently Installed Segments

Type	Name	Version	Class	Size	Disk
S/W	COE Component Parent	1.0.0.2	U	2.93 MB	/h
S/W	Password	1.0.0.0	U	6.84 MB	/h
S/W	X Display Manager	1.0.0.0	U	0.69 MB	/h
S/W	Console Window	1.0.0.1	U	1.84 MB	/h
S/W	Deadman	1.0.0.1	U	0.23 MB	/h

Select Software To Install

Type	Name	Version	Class	Size	Disk
S/W	Sample Aggregate Segment	1.0.0.0	U	0.12 MB	/h
ACCTGRP	Sample Account Group Segment	1.0.0.0	U	0.07 MB	/h
COTS	Sample COTS Segment	1.0.0.0	U	0.02 MB	/h
DATA	Sample Data-Global Segment	1.0.0.0	U	0.02 MB	/h

Figure 15. Installer Window with Select Software To Install Panel

`Available Disks`

Displays the mounted disk drives on the system and the remaining available disk space. The amount of available disk space decreases as segments are selected for installation. This panel has five fields: `Disk`, `Actual`, `Available`, `Selected`, and `Reserved`.

`Disk`

Shows each available disk.

`Actual`

Shows the total size of each disk.

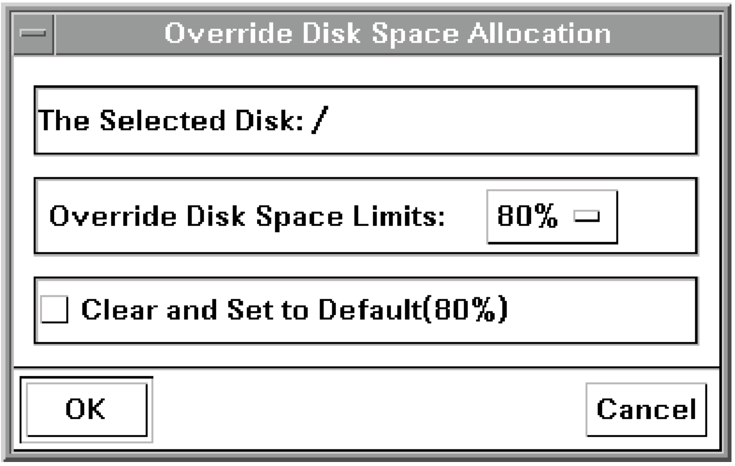
`Available`

Shows the free space that is available on each disk for installing segments.

`Selected`
Shows the size of the segment(s) you want to add or remove based on your selection of one or more segments in the `Currently Installed Segments` panel.

`Reserved`
Shows the amount of space on each disk that is already in use or pre-allocated (reserved) by previously installed segments.

The `Available Disks` panel has the following button: `Reserved Space`. The system automatically reserves a certain amount of space on each available disk to allow for segment growth. The `Reserved Space` button allows the reserved disk space to be modified for a particular installation. To modify reserved disk space for a particular installation, click on a disk in the list to highlight it and then click on the `Reserved Space` button to open the `Override Disk Space Allocation` window (Figure 16). The `Override Disk Space Limits` pop-up menu allows the user to choose between 80 percent and 100 percent of space to install the segment.


Override Disk Space Allocation

The Selected Disk: /

Override Disk Space Limits: 80%

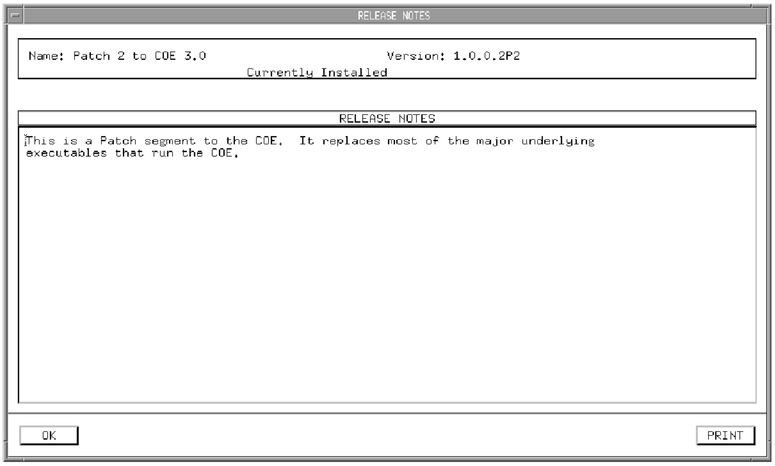
□ Clear and Set to Default(80%)

Figure 16. Override Disk Space Allocation Window

`Currently Installed Segments`
Lists the segments that are currently installed. The `Currently Installed Segments` panel lists the type, name, version number, classification, size, and disk (mount point) of each currently installed segment. This panel has two buttons: `Release Notes` and `Deinstall Software`.

`Release Notes`
Displays release notes information for any selected segment. Click on a segment to highlight it and click on the `Release Notes` button to open the `RELEASE NOTES` window (Figure 17). Click on the `PRINT` button to print the release notes.

`Deinstall Software`
Allows the user to deinstall segments highlighted in the `Currently Installed Segments` panel.



Name: Patch 2 to COE 3.0 Version: 1.0.0.2P2

Currently Installed

RELEASE NOTES

This is a Patch segment to the COE. It replaces most of the major underlying executables that run the COE.

Figure 17. RELEASE NOTES Window

`Select Software To Install`

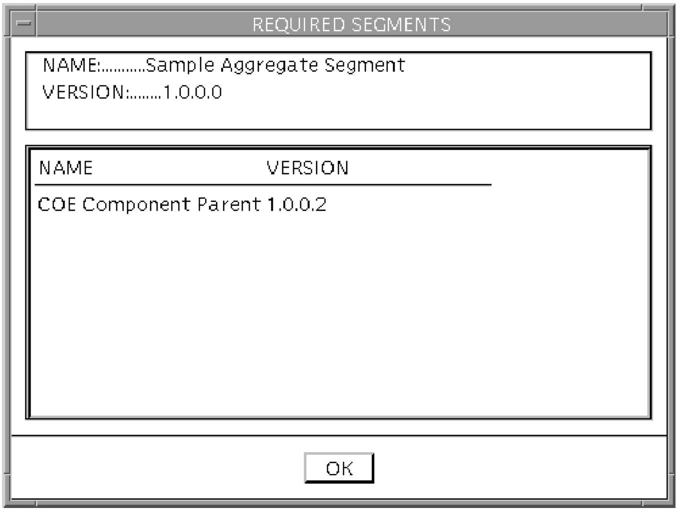
Lists the segments that are contained on the selected media and that are not currently installed. The `Select Software To Install`panel lists the type, name, version number, classification, size, and mount point (disk) of each segment contained on the media. This panel has five buttons: `Release Notes`, `Requires`, `Conflicts`, `Install`, and `Exit`.

`Release Notes`

Displays release notes information for any selected segment. Click on a segment to highlight it and click on the `Release Notes` button to open the `RELEASE NOTES` window (Figure 17). Click on the `PRINT` button to print the release notes.

`Requires`

Lists segments that need to be installed in order to install the segment selected in the `Select Segment To Install`panel. Click on a segment to highlight it and click on the `Requires` button to open the `REQUIRED SEGMENTS` window (Figure 18).

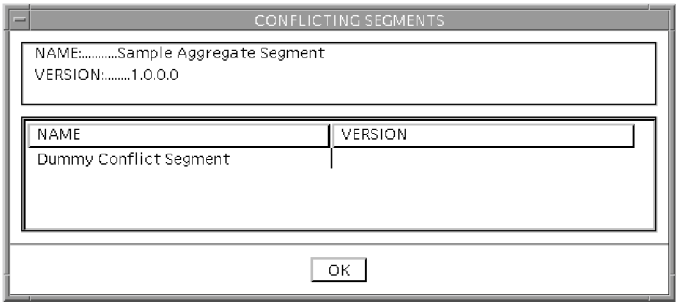


NAME:..........Sample Aggregate Segment
VERSION:........1.0.0.0

NAME	VERSION
COE Component Parent	1.0.0.2

Figure 18. REQUIRED SEGMENTS Window

`Conflicts`
Lists the segments that cannot be installed with the segment selected in the `Select Segment To Install` panel. Click on a segment to highlight it and click on the `Conflicts` button to open the `CONFLICTING SEGMENTS` window (Figure 19).


CONFLICTING SEGMENTS

NAME:..........Sample Aggregate Segment
VERSION:........1.0.0.0

NAME	VERSION
Dummy Conflict Segment	

Figure 19. CONFLICTING SEGMENTS Window

`Install`
Allows the user to install selected segments.

`Exit`
Exits the user from the `Installer` window.

6.3.1.3 Installing Segments

Follow the steps below to install segments using the `Segment Installer` option.

STEP 1: **Select the installation device**. Click on the `Select Source` button in the `Source` panel to open the `Select Source` window (Figure 14). Select the device to use as the installation source device. Select `NETWORK` if you are installing a segment from the segment installation server. Refer to Section 6.3.2, *Segment Installation Server Option*, for information about loading segments on the segment installation server.

STEP 2: **Read the table of contents of the selected installation device**. Click on the `Read Contents` button in the `Source` panel. The media will be scanned for the segments that it contains, and then the `Installer` window will add the `Select Software To Install` panel, which lists the segments that the media contains (Figure 15). Any number of segments may be selected in this panel for installation.

STEP 3: **Select the segments that you want to install**. Click on one or more segments in the `Select Software To Install`panel. The `Available Disks` panel then displays the mounted disk drives on the system and the remaining available disk space as segments are selected.

STEP 4: **Begin the installation process for the selected segments**. Click on the `Install` button once all desired segments are selected. The `Installer Status` window appears, which shows the number of segments to be installed and the size of each segment being installed. This window also shows a `Percent Complete` status bar, which shows the status of the installation.

STEP 5: **Display a detailed log of the installation process**. Select the `Installation Log` option from the `Installed` pull-down menu once installation has completed.

6.3.2 Segment Installation Server Option

The `Segment Installation Server` option is used to load segments onto a segment server. Loading a segment is different than installing a segment. Loading a segment on a machine stores the segment on the machine, but does not enable the segment to run. Instead, segments stored on a segment installation server are available for installation without the installation media because they are located on a server. Segments can, then, be installed individually on each machine on the network.

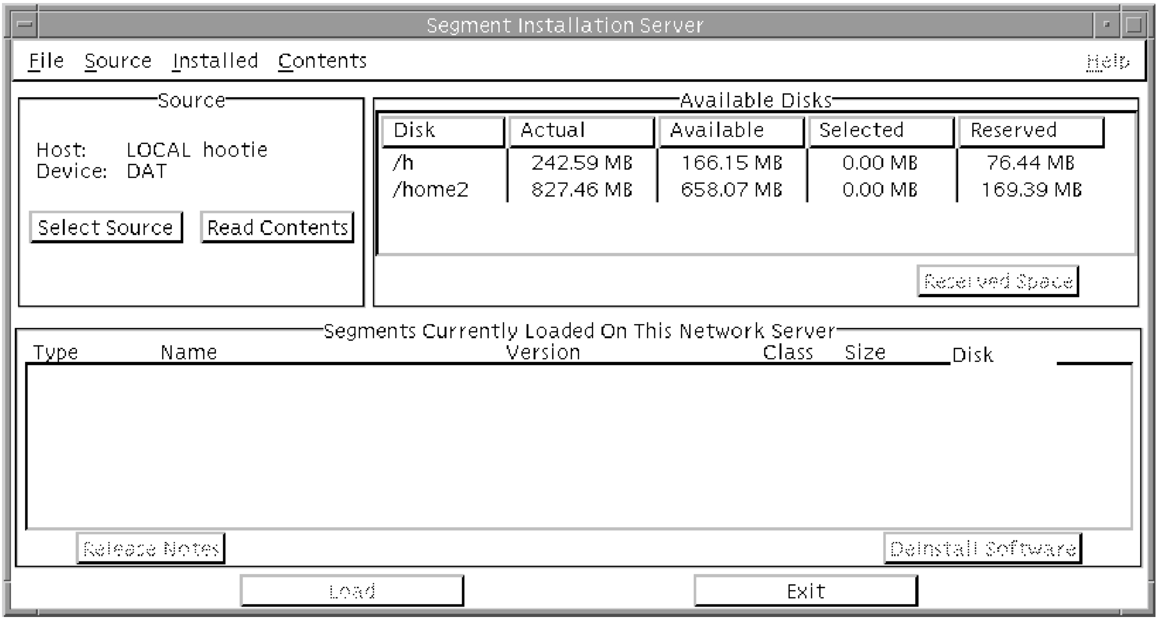
Click on the `Segment Installation Server` option to open the `Segment Installation Server` window (Figure 20). This window is identical to the `Installer` window, with the following exceptions:

C The `Load` option in the `File` pull-down menu replaces the `Install` option.

C The `Load` button replaces the `Install` button.

C The `Segments Currently Loaded On This Network Server` panel replaces the `Currently Installed Segments` panel.

NOTE: Ensure that you can see the whole window by clicking on the bottom right edge of the window and dragging the trackball or mouse outward to enlarge the window.



Host: LOCAL hootie
Device: DAT

Disk	Actual	Available	Selected	Reserved
/h	242.59 MB	166.15 MB	0.00 MB	76.44 MB
/home2	827.46 MB	658.07 MB	0.00 MB	169.39 MB

Figure 20. Segment Installation Server Window

6.3.2.1 Loading Segments on the Segment Installation Server

NOTE: The following must be done for the network installation to be successful:

C The `/h/data/global` directory must be mounted to a common machine. If `/h/data/global` is not mounted, use the `Disk Manager` option from the `Hardware` pull-down menu to mount it (see Subsection 6.2.3, *Disk Manager Option*).

C Segments installed from a segment installation server must have been loaded on `/home2` or on any other exported file system on the server machine; if they are not, the COEInstaller will not be able to access the segments. The machine that the segments are being installed from must be in the target machine's host file or, if running DNS, then the host must be in the DNS file.

Follow the steps below to load a segment on the segment installation server.

STEP 1: **Select a server on which to load segments**. Select a disk in the `Available Disks` panel. A list of segments, which can be installed from the `Installer` window, is created automatically in the `/h/data/global` directory and is updated each time a segment is loaded using this option.

STEP 2: **Select the installation device**. Click on the `Select Source` button in the `Source` panel to open the `Select Source` window (Figure 14). Select the installation source device and then click on the `OK` button.

STEP 3: **Select the segments that you want to load**. Click on one or more segments in the `Select Software To Install` panel. The `Available Disks` panel then displays the mounted disk drives on the system and the remaining available disk space as segments are selected.

STEP 4: **Begin the load process for the selected segments**. Click on the `Load` button once all desired segments are selected. The `Installer Status` window appears, which shows the number of segments to be loaded and the size of each segment being loaded. This window also shows a `Percent Complete` status bar, which shows the status of the load.

STEP 5: **Display a detailed log of the load process**. Select the `Installation Log` option from the `Installed` pull-down menu once the load has completed.

Follow the steps in Section 6.3.1.3, *Installing Segments*, to install one or more segments on a machine.

6.4 Network Menu

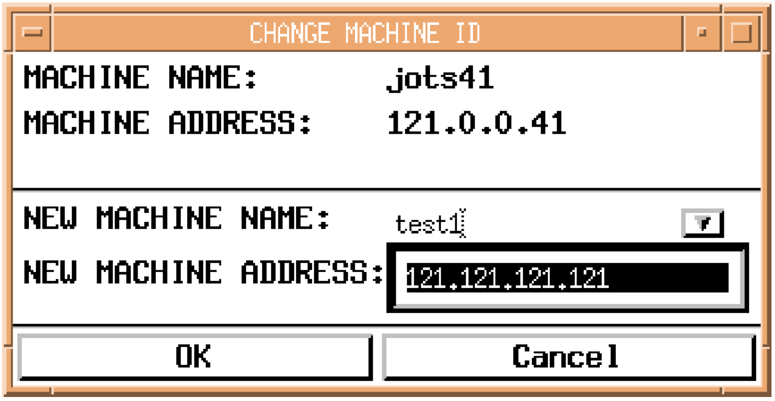
The `Network` menu contains the following options: `Change Machine ID`, `Edit Local Hosts`, `Set System Time`, `Servers`, and `DCE`. These options are described in the following subsections.

6.4.1 Change Machine ID Option

Use the `Change Machine ID` option to select a name and IP address for a machine. Click on this option to open the `CHANGE MACHINE ID` window (Figure 21). The machine's current name and IP address appear in the `MACHINE NAME` and `MACHINE ADDRESS` fields.

NOTE: A machine's name (ID) and IP address are selected initially during system installation.

NOTE: All machines must have unique names and addresses—the system does not permit two machines to have the same name and address.


CHANGE MACHINE ID

MACHINE NAME: jots41

MACHINE ADDRESS: 121.0.0.41

NEW MACHINE NAME: test1

NEW MACHINE ADDRESS: 121.121.121.121

Figure 21. CHANGE MACHINE ID Window

Follow the steps below to change the machine ID.

STEP 1: **Select a new machine**. Click on the arrow to the right of the `NEW MACHINE NAME` field to display a pop-up list of valid IDs.

STEP 2: **Select an ID.** Click on an ID to select it.

> **NOTE**: User-defined names may be assigned to each machine using the `Edit Local Hosts` option before changing the machine ID (see Subsection 6.4.2, *Edit Local Hosts Option*).

STEP 3: **Click on the `OK` button**. The `MACHINE NAME` and `MACHINE ADDRESS` fields update to reflect the new machine name and address.

STEP 4: **Reboot the machine**. Reboot the machine after changing the name for the change to take effect.

> **NOTE**: Do not modify the `NEW MACHINE ADDRESS` field. Machine addresses are predefined for each ID.

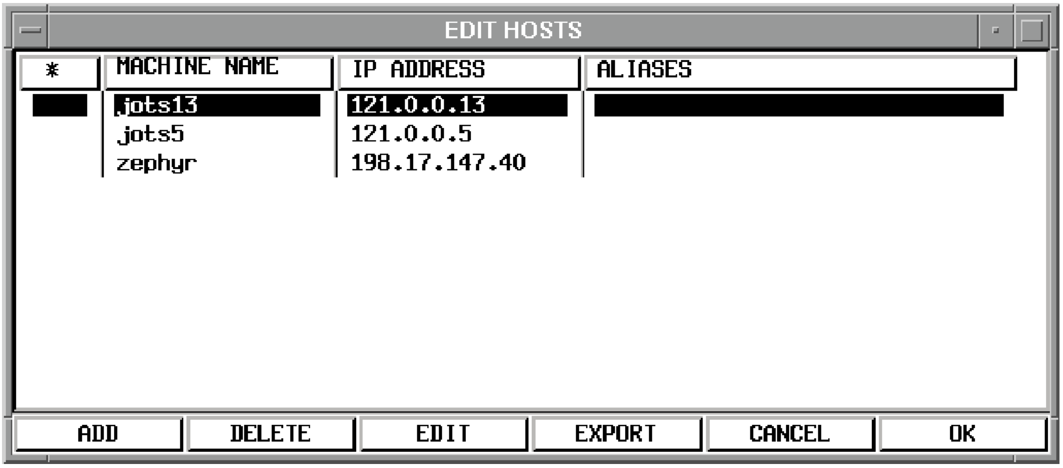
6.4.2 Edit Local Hosts Option

The `Edit Local Hosts` option lists the machines that can be accessed from a user's machine. This option can only be used on local workstation files. Use this option to do the following:

- Add or remove machines from the list of machines that can be accessed

- Modify machine information, such as machine name, IP address, or aliases.

Select the `Edit Local Hosts` option to open the `EDIT HOSTS` window (Figure 22).



*	MACHINE NAME	IP ADDRESS	ALIASES
	jots13	121.0.0.13	
	jots5	121.0.0.5	
	zephyr	198.17.147.40	

Figure 22. EDIT HOSTS Window

Follow the steps below to modify machine information. These steps must be performed for each machine you want to modify.

STEP 1: **Modify host file information**. Use the Edit Local Hosts option to add or remove machines from the list or to modify machine information. Once you have completed the selected action, the machine remains in the EDIT HOSTS window labeled with A (add), M (modify), or D (delete) in the * column. Click on the OK button to accept the changes, or click on the CANCEL button to discard the changes.

STEP 2: **Assign the machine a new machine name**. Assign the machine a new machine name using the Change Machine ID option (see Subsection 6.4.1, *Change Machine ID Option*).

STEP 3: **Reboot the machine**. Reboot the machine at the prompt if you modified the current hostname in order for changes to take effect.

6.4.2.1 EDIT HOSTS Window Fields

The EDIT HOSTS window has the following fields: * (asterisk), MACHINE NAME, IP ADDRESS, and ALIASES. These fields are described below.

*** (asterisk)**
Shows pending changes made to the machine. Labels include A (add), D (delete), M (modify), and T (trusted).

The label T indicates a trusted machine. A trusted machine can be accessed from another machine on the same LAN (e.g., to access a tape drive for remote installation). A trusted machine is one that can access the user's disk and perform remote shell commands.

MACHINE NAME
Shows the name of the machine. The machine name can be system or user defined.

IP ADDRESS
Shows a unique IP address.

ALIASES
Shows other names by which a machine is also known, if applicable.

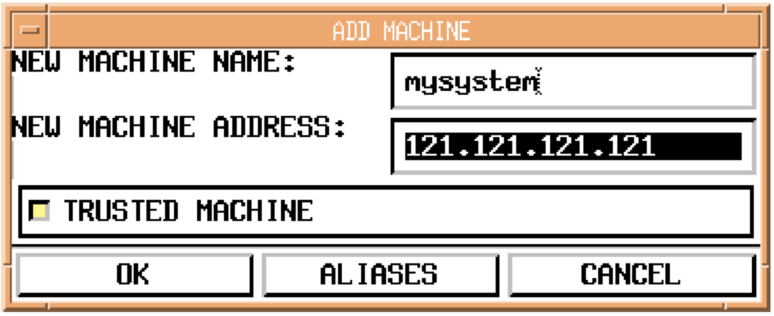
6.4.2.2 EDIT HOSTS Window Buttons

The EDIT HOSTS window has the following buttons: ADD, DELETE, EDIT, EXPORT, CANCEL, and OK. These buttons are described below.

ADD

Used to add a machine to the local host table to make it available to the local machine. Follow the steps below to add a machine to the local host table.

STEP 1: **Click on the ADD button**. The ADD MACHINE window appears (Figure 23).



NEW MACHINE NAME: mysystem

NEW MACHINE ADDRESS: 121.121.121.121

Figure 23. ADD MACHINE Window

STEP 2: **Enter the new machine name**. Type a name in the NEW MACHINE NAME field. Allowable characters are alphanumeric and the underscore symbol (_). In addition, the first character of the machine name must be a letter.

STEP 3: **Enter the machine's IP address**. Type the IP address of the new machine in the NEW MACHINE ADDRESS field.

STEP 4: **Define the new machine as a trusted machine**. Click on the TRUSTED MACHINE checkbox toggle.

STEP 5: **Add aliases for a machine, if desired**. Click on the ALIASES button in the ADD MACHINE window to open the ALIASES window (Figure 24).

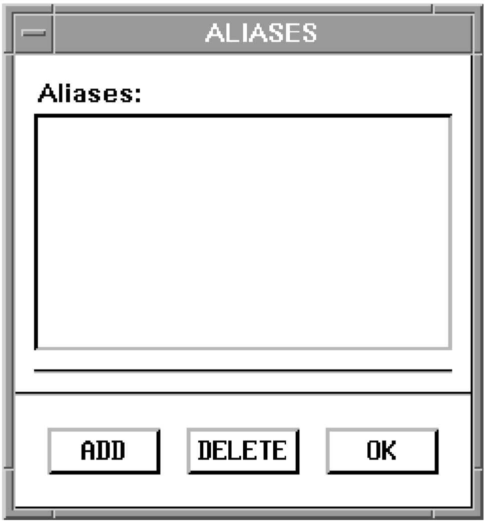
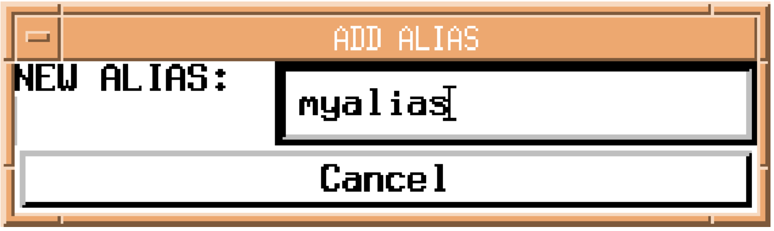


Figure 24. ALIASES Window

To add an alias, click on the ADD button. The ADD ALIAS window appears (Figure 25). Type a new alias in the NEW ALIAS field and then press [RETURN] to accept the new alias. Allowable characters are alphanumeric and the underscore symbol (_). In addition, the first character of the machine name must be a letter. The ALIASES window reappears.



myalias

Figure 25. ADD ALIAS Window

STEP 6: **Close the ALIASES window and save the changes**. Click on the OK button. The ADD MACHINE window returns to the forefront.

STEP 7: **Determine if the machine should be added to the list of available machines**. Click on the OK button to mark the machine as an addition to the list of available machines on the local host table, or click on the CANCEL button to discard the changes. The ADD MACHINE window closes.

DELETE
Used to delete a machine from the local host table. Follow the steps below to delete a machine from the local host table.

STEP 1: **Select a machine**. Click on a machine in the list to highlight it.

STEP 2: **Click on the DELETE button**. The DELETE MACHINE dialog box appears with the following prompt: `Mark machine [machine name] for deletion?`

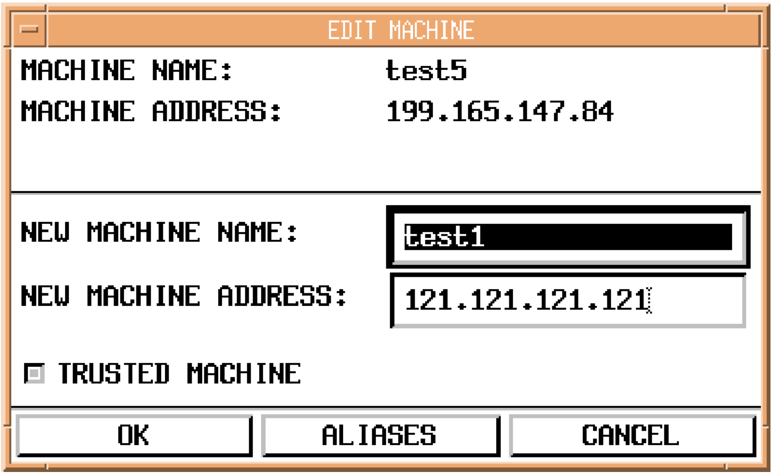
STEP 3: **Confirm whether or not the machine should be deleted**. Click on the YES button to confirm that the machine should be deleted, or click on the NO button to cancel the deletion.

EDIT
Used to edit a machine name. Click on a machine name to highlight it and click on the EDIT button to open the EDIT MACHINE window (Figure 26). The EDIT MACHINE window functions the same as the ADD MACHINE window (described in **ADD**).

EXPORT
Used to export machine information to other workstations on the local host table. (Not currently implemented.)

CANCEL
Used to close the EDIT HOSTS window without saving changes.

OK
Used to save changes and close the window.

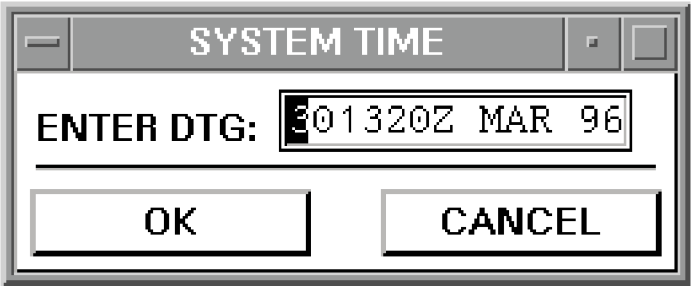


MACHINE NAME: test5
MACHINE ADDRESS: 199.165.147.84
NEW MACHINE NAME: test1
NEW MACHINE ADDRESS: 121.121.121.121
☑ TRUSTED MACHINE

Figure 26. EDIT MACHINE Window

6.4.3 Set System Time Option

The `Set System Time` option is used to set the system time for the machine. Click on the `Set System Time` option to open the `SYSTEM TIME` window (Figure 27).



ENTER DTG: 301320Z MAR 96

Figure 27. SYSTEM TIME Window

The system time is written as ddhhmmZ MON YR, where

dd	=	day of the month
hh	=	hour
mm	=	minute
Z	=	a constant (for Zulu time)
MON	=	three-letter month abbreviation
YR	=	final two digits of the year.

For example, October 15, 1996, 8:19 Zulu time would read: 150819Z OCT 96.

To set the system time, follow the steps below:

STEP 1: **Enter the new system time**. Enter the new system time in the `ENTER DTG` field in the format ddhhmmZ MON YR.

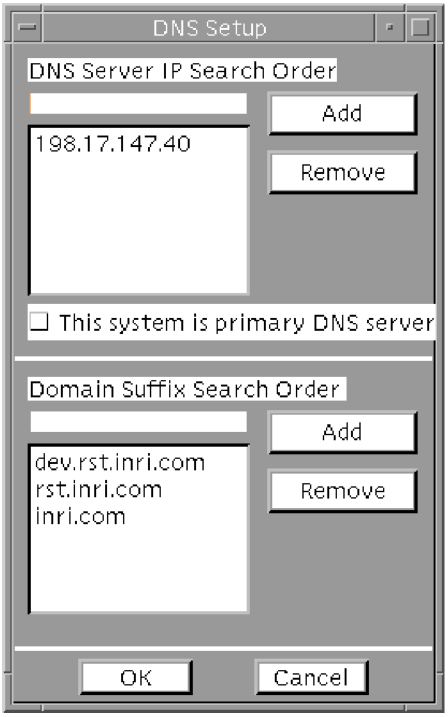
STEP 2: **Set the new system time for the machine**. Click on the `OK` button to accept the new entry, or click on the `CANCEL` button to discard the entry.

6.4.4 Servers Option

The `Servers` option is a cascading menu that has four options: `Set DNS`, `Set Routes`, `Set Mail`, and `Set NIS`. These options are described in the following subsections.

6.4.4.1 Set DNS Option

The `Set DNS` option allows the system administrator to configure a workstation as either a Domain Name Server (DNS) client or a DNS server if DNS, rather than the local host table, is used to store host name IP address information. Figure 28 shows the `DNS Setup` window. The `Set DNS` option creates the nameserver configuration file upon a positive response. If the `This system is primary DNS server`toggle is checked, the Set DNS option installs a set of DNS template files to `/var/nameserver`. This function allows the system administrator to enter the IP address of the primary and secondary name servers. It also allows the system administrator to specify suffixes of machine names instead of IP addresses, as well as specify domain name suffixes of machines for the local domain instead of IP addresses.



DNS Server IP Search Order

198.17.147.40

□ This system is primary DNS server

Domain Suffix Search Order

dev.rst.inri.com
rst.inri.com
inri.com

Figure 28. DNS Setup Window

NOTE: The system administrator must edit the /var/nameserver DNS template files manually for proper name server configuration.

NOTE: On Solaris 2.x Operating Systems, a new /etc/nsswitch.conf file with the appropriate reference to DNS will be installed. The only change to this file is that the DNS references are added. On HP Operating Systems, a new /etc/resolv.conf file will be installed that includes the DNS name server list and the domain search list.

If your workstation is acting as the primary DNS server, click on the Add button to enter the IP address of the DNS server in the DNS Server IP Search Order field and click on the This system is primary DNS server toggle. You can also click on the Add button to enter the IP address of a backup DNS server in the DNS Server IP Search Order field. In addition, you can click on the Add button to add multiple domain suffixes in the Domain Suffix Search Order field. A domain suffix is a list of suffixes appended to a system name that are used to help locate the system. Click on the OK button when finished.

If your workstation is not acting as the primary DNS server, click on the Add button to enter the IP address of the primary DNS server in the DNS Server IP Search Order field and then enter the IP address of the backup DNS server. Do NOT click on the This system is primary DNS server toggle. You can also click on the Add button to add multiple domain suffixes in the Domain Suffix Search Order field. Click on the OK button when finished. The DNS domain name must match the DNS domain for the name server.

6.4.4.2 Set Routes Option

The Set Routes option allows the system administrator to configure a workstation with the appropriate default routing configuration. Select this option to open the Default Router Setup window (Figure 29). If your workstation is acting as the default router, enter the IP address of the default router in the Default Router IP Address field and click on the This system is default router toggle. If your workstation is not acting as the default router, enter the IP address of the default router in the Default Router IP Address field. Do NOT click on the This system is default router toggle. Click on the OK button when finished.

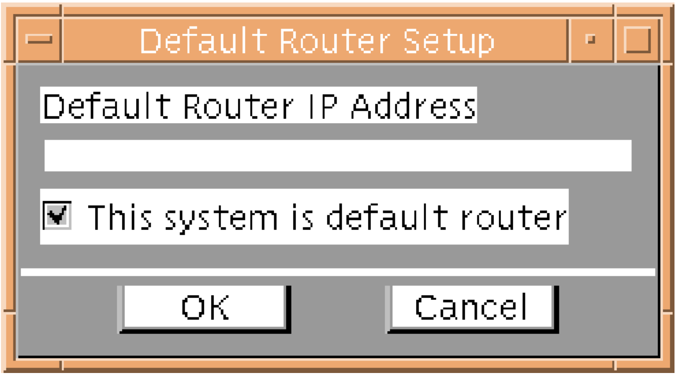


Figure 29. Default Router Setup Window

NOTE: The default router only needs to be configured for access to networks other than the LAN. The default router may also be configured during kernel installation.

6.4.4.3 Set Mail Option

The `Set Mail` option allows the system administrator to configure mail on a workstation as either a client or a server. Select the `Set Mail` option to open the `Mail Setup` window (Figure 30). This option creates the `/etc/lib/sendmail.cf` file, which is a configuration file used for sending mail. Clicking on the `OK` button adds an entry into the operating system-specific mount configuration table.

If your workstation is acting as the mail server, enter the mail server IP address in the `Default Router IP Address` field and click on the `This system is mail server` toggle. If your workstation is not acting as the mail server, enter the mail server IP address in the `Default Router IP Address` field. Do NOT click on the `This system is mail server` toggle. Click on the `OK` button when finished.

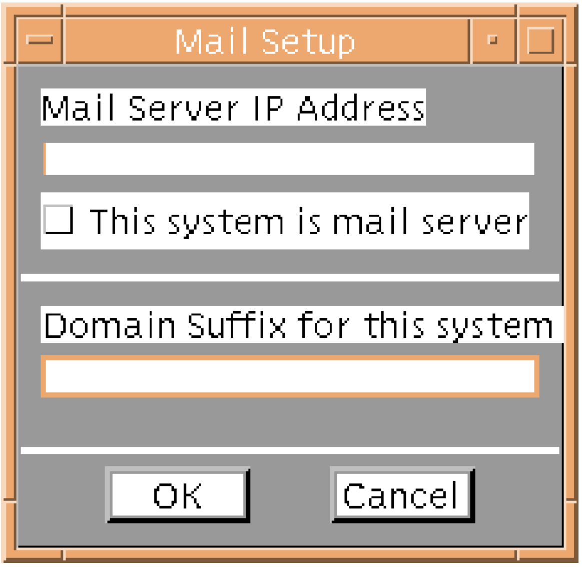


Figure 30. Mail Setup Window

NOTE: The `Set Mail` option is not available on HP workstations.

6.4.4.4 Set NIS Option

Network Information Service (NIS) allows user accounts to be shared across all workstations on the same domain. The `Set NIS` option is used to initialize a machine as a NIS server, add client workstations to the NIS domain, and disable NIS. The `Set NIS` option is a cascading menu that has three options: `Initialize NIS`, `Add NIS Client`, and `Remove NIS`.

Before NIS can be initialized, DNS should be configured on the master server and on the client machine. Refer to Section 6.4.4.1, *Set DNS Option*, for information on configuring DNS. In addition, an entry must be added to export the global users directory before NIS can be initialized. In other words, one workstation on the NIS master must have `/h/USERS/global` exported (shared) as read/write and must have `anon=0` to allow root access. If `/h/USERS/global` is not mounted, use the `Disk Manager` option from the `Hardware` pull-down menu to mount it, as described in the next subsection.

To initialize NIS, you need to know the NIS domain name, the client host name and client IP address, the NIS server host name, and the network password (also known as the Secure-RPC password). Your system administrator should provide you with this information.

Adding an Entry To Export the Global Users Directory

Follow the steps below to add an entry to export the global users directory.

STEP 1: **Open the `Disk Manager` window**. Select the `Disk Manager` option from the `Hardware` pull-down menu. The `Disk Manager` window appears (Figure 8).

STEP 2: **Select a file system**. Click on a file system in the list to highlight it and then click on the `EXPORTFS` button. The `Export/Unexport File Systems` window appears (Figure 12).

STEP 3: **Enter the appropriate options**. Type `rw,anon=0` in the `options` field to export the global users directory.

STEP 4: **Enter the appropriate pathname**. Type `/h/USERS/global` in the pathname field.

STEP 5: **Export the file system**. Click on the `Export` button.

STEP 6: **Export the file system permanently**. (Solaris only) Click on the `Yes` button when the following prompt appears: `Do you want to permanently export the file system?` The window closes.

STEP 7: **Confirm that the file was exported**. Click on the `Current` button in the `Disk Manager` window. The `/h/USERS/global` directory should appear in the list of exported file systems.

NOTE: Refer to Subsection 6.2.3, *Disk Manager Option*, for more information on mounting and exporting file systems.

Initializing NIS on the Master or the Client

Follow the steps below to initialize NIS on the master or the client machine.

NOTE: On an HP workstation, C2 must be disabled before initiating NIS. This can be done by running `/etc/tsconvert -r` and by disabling the auditing monitor daemon from the `/etc/rc.config.d/auditing` file. To do this, change `AUDITING=1` to `AUDITING =0`.

NOTE: It is recommended that the master server be initialized before any client machines.

STEP 1: **Initialize NIS**. Select the `Initialize NIS` option from the `Set NIS` cascading menu option.

STEP 2: **Enter the NIS domain name**. An `ENTER A RESPONSE` window appears. Enter the domain name at the prompt and click on the `OK` button or press [`RETURN`]. This is the name of the domain that will include the master and client machines.

NOTE: The NIS domain name must contain two parts separated by a `.` (period).

STEP 3: **Set the machine as the master server or as a client**. The `RESPOND TO THE QUESTION` window appears with the following prompt: `Is this machine the Master NIS Server?` If the machine is the client, click on the `No` button and proceed to STEP 4; if the machine is the server, click on the `Yes` button and proceed to STEP 10.

STEP 4: **Enter the NIS server host name**. The `ENTER A RESPONSE` window appears with the following prompt: `Enter the NIS Server Host Name`. Enter the name of the machine designated as the server at the prompt and click on the `OK` button or press [`RETURN`].

STEP 5: **Acknowledge that the NIS server host is reachable**. An `INFORMATIONAL MESSAGE` window appears with the following message: `[NIS Server Host Name] is reachable`. Click on the `OK` button or press [`RETURN`].

STEP 6: **Continue the initialization**. The following message appears:

```
Initializing client [client name] for domain [domain name]
Once initialization is done, you will need to reboot your
machine. Do you want to continue?
```

Type `Y` and press [`RETURN`] to continue, or type `N` and press [`RETURN`] to exit the script. If you type `Y`, proceed to STEP 7; if you type `N`, proceed to STEP 10.

STEP 7: **Enter the network password**. (Solaris only) Several messages appear, ending with the following:

```
At the prompt below, type the network password (also known as
the Secure-RPC password) that you obtained either from your
administrator or from running the nispopulate scripts.
Please enter the Secure-RPC password for root:
```

Enter a password described in the NOTE on the next page and press [`RETURN`].

STEP 8: **Enter the login password for root**. (Solaris only) Enter a password at the prompt and press [`RETURN`]. The following message appears: `Your network has been changed to your login one. Your network and login passwords are now the same.` Proceed to STEP 10.

NOTE: (Solaris only) This password remains in the password file even if NIS is removed from the client machine. The following message will appear if NIS has already been configured and if the password has already been entered.

```
If the machine was initialized before as a NIS+ client, please enter the
root login password as the network password. Or re-type the network
password that your administrator gave you.
```

Enter the appropriate password and press [`RETURN`]. The following message appears:

```
Your network has been changed to your login one. Your network and login
passwords are now the same.
```

STEP 9: **Enter and confirm a secman password**. The `ENTER A PASSWORD` window appears after several minutes. Enter a secman password and press [`RETURN`]. Re-enter the password to verify it and press [`RETURN`]. Then click on the `OK` button.

STEP 10: **Enter and confirm a sysadmin password**. The `ENTER A PASSWORD` window appears after several minutes. Enter a sysadmin password and press [`RETURN`]. Re-enter the password to verify it and press [`RETURN`]. Then click on the `OK` button.

STEP 11: **Acknowledge that the machine needs to be rebooted**. An `INFORMATIONAL MESSAGE` window appears with the following message: `Please Reboot this machine`. Click on the `OK` button to close the window.

STEP 12: **Reboot the machine**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?`Click on the `OK` button to reboot the machine.

NOTE: The system takes several minutes to reboot. During this time, several informational messages appear, including the following:

```
NIS domainname is [domain name]
```

The domain name will be the name you specified in STEP 2. This message confirms that NIS has been initialized on the machine.

NOTE: The following message also appears on the master server ONLY upon this initial reboot:

```
The password used will be nisplus
Use this password when the nisclient script requests the network
password.
```

This is the password to be entered in STEP 7 when NIS is initialized on the client machine.

When the reboot is complete, the DII COE Login window appears. NIS is configured.

Adding a NIS Client

Follow the steps below to add a machine as a NIS client. This section applies to Solaris only.

NOTE: NIS clients can only be added on the master server machine.

NOTE: When adding a NIS client, the server and client must recognize each other through inclusion in the local hosts table.

STEP 1: **Select the `Add NIS Client` option**. Select the `Add NIS client` option from the `Set NIS` cascading menu option on the NIS server.

STEP 2: **Enter the client host name**. The `ENTER A RESPONSE` window appears. Enter the client host name at the prompt and click on the `OK` button.

STEP 3: **Enter the client IP address**. The `ENTER A RESPONSE` window appears. Enter the IP address at the prompt and click on the `OK` button.

STEP 4: **Enter and confirm the client `root` password**. The `ENTER A PASSWORD` window appears. Enter the root password and press [RETURN]. Re-enter the password to verify it and press [RETURN]. Then click on the `OK` button.

STEP 5: **Determine if you want to initialize the machine as a client**. The following prompt appears:

```
Initializing client [name] for domain “.”. Once initialization
is done, you will need to reboot your machine. Do you wish to
continue?
```

Type `Y` or `N` and press [RETURN]. The window closes.

STEP 6: **Reboot the machine**. Reboot the machine if you added a NIS client. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?` Click on the `OK` button to reboot the machine.

NOTE: No message appears to tell you if the process was successful.

Removing NIS

The `Remove NIS` option disables NIS from the system, which removes the domain name and, upon reboot, does not start NIS processes. Follow the steps below to disable and remove NIS.

STEP 1: **Select the `Remove NIS` option**. Select the `Remove NIS` option from the `Set NIS` cascading menu option.

STEP 2: **Disable and remove NIS**. The `ENTER A RESPONSE` window appears with the following message: `Do you wish to disable and remove NIS?`Click on the `No` button to close the window, or click on the `Yes` button to disable and remove NIS.

NOTE: No message appears to tell you if the process was successful.

STEP 3: **Acknowledge that the machine needs to be rebooted**. (HP only) An informational message appears prompting you to reboot the machine. Click on the `OK` button.

STEP 4: **Reboot the machine**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?`Click on the `OK` button to reboot the machine.

NOTE: The system takes several minutes to reboot. During this time, several informational messages appear, including the following:

```
NIS domainname is
```

This domain name field will be blank if NIS was removed successfully.

The system reboots to the DII COE Login screen.

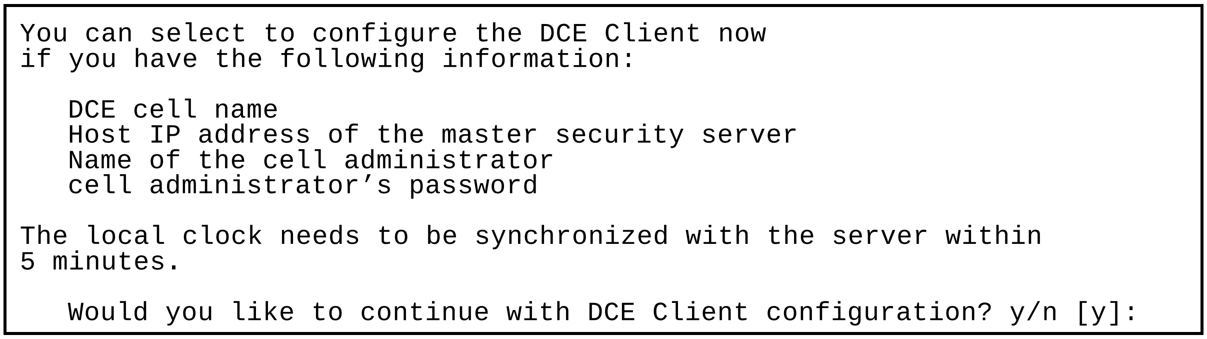
NOTE: If you want to enable NIS, reboot the workstation first, then initialize NIS.

6.4.5 DCE Option

The `DCE` option is a cascading menu that has four options: `Configure DCE Client`, `Configure DTS server`, `Configure Audit server`, and `Unconfigure DCE`. These options are described in the following subsections.

6.4.5.1 Configure DCE Client Option

The `Configure DCE Client` option allows the system administrator to configure a workstation as a client system in a DCE cell. Select the `Configure DCE Client` option to open the `DCE Client Configuration` screen (Figure 31).



```
You can select to configure the DCE Client now
if you have the following information:

   DCE cell name
   Host IP address of the master security server
   Name of the cell administrator
   cell administrator’s password

The local clock needs to be synchronized with the server within
5 minutes.

   Would you like to continue with DCE Client configuration? y/n [y]:
```

Figure 31. DCE Client Configuration Screen

DCE is normally configured during initial system installation; however, DCE configuration can be skipped during the system installation process. Refer to the *DII COE Kernel Installation Guide (Solaris 2.5.1)* for information about configuring the DCE client during initial system installation.

The `Configure DCE Client` option allows DCE client configuration to be performed after the initial installation. The interface is through a series of prompted questions and responses from a terminal window.

NOTE: The local clock *MUST* be synchronized to within 5 minutes of the server clock for the system to configure DCE. If the times are not synchronized, DCE configuration will fail.

NOTE: You must unconfigure DCE before attempting to configure DCE.

NOTE: Do not continue with the client configuration if a server is not configured and operating.

NOTE: If the system is configured into a cell, you must reconfigure the system before starting the DCE client configuration.

Follow the steps below to configure a workstation as a client system in a DCE cell.

STEP 1: **Determine if you would like to continue with the DCE client configuration**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 2: **Enter the cell name**. Enter the cell name at the prompt and press [RETURN].

STEP 3: **Enter the Internet Protocol (IP) address of the master security server**. Enter the IP address at the prompt and press [RETURN].

STEP 4: **Enter the name of the cell administrator**. Enter the name of the cell administrator at the prompt and press [RETURN].

STEP 5: **Enter the cell administrator's password**. Enter the password at the prompt and press [RETURN].

STEP 6: **Determine if you would like to configure this node as a DFS client server**. Type `Y` or `N` at the prompt and press [RETURN]. If you are on an HP workstation, proceed to STEP 7; if you are on a Sun workstation, proceed to STEP 11.

STEP 7: **Determine where the cache is located**. The following prompt appears: `Is the cache: 1. in memory 2. on the local drive.`Type `1` or `2` and press [RETURN].

STEP 8: **Enter the size of the cache**. The following prompt appears: `Enter size of cache (10000)`. Enter a new cache size or press [RETURN] to accept the default value.

STEP 9: **Determine the cache directory**. The following prompt appears: `Enter the name of the cache directory (/opt/dcelocal/var/adm/dfs/cache)`. Enter a directory name or press [RETURN] to accept the default directory.

STEP 10: **Determine if the DFS client is to be configured as an NFS gateway**. The following prompt appears: `Would you like to configure this DFS client as an NFS gateway?` Type `N` and press [RETURN].

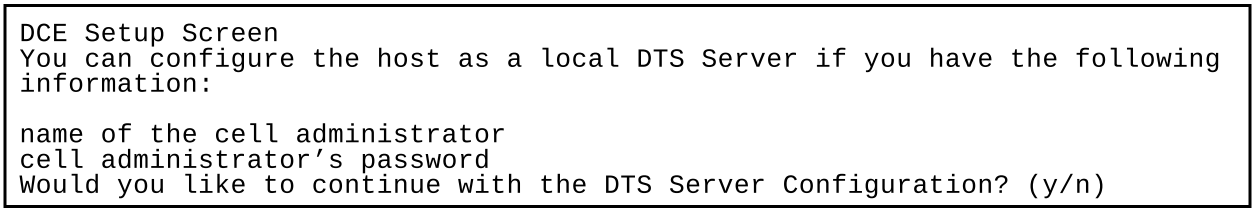
STEP 11: **Determine if you would like to configure this node as a local DTS server**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 12: **Determine if you would like to configure this node as an audit server**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 13: **Exit the DCE client configuration display**. Type `q` at the prompt and press [RETURN] to exit the DCE client configuration display.

6.4.5.2 Configure DTS Server Option

The `Configure DTS server` option allows the system administrator to configure the host as a local DTS server. Select the `Configure DTS server` option to open the `DCE Server Configuration` screen (Figure 32).



```
DCE Setup Screen
You can configure the host as a local DTS Server if you have the following
information:

name of the cell administrator
cell administrator’s password
Would you like to continue with the DTS Server Configuration? (y/n)
```

Figure 32. DCE Server Configuration Screen

Follow the steps below to configure the host as a local DTS server.

STEP 1: **Determine if you want to continue with the DTS server configuration**. Type `Y` or `N` and press [RETURN].

STEP 2: **Enter the name of the cell administrator**. Enter the name at the prompt and press [RETURN].

STEP 3: **Confirm the name of the cell administrator**. Enter the name again and press [RETURN].

STEP 4: **Enter the cell administrator’s password**. Enter the password at the prompt and press [RETURN].

STEP 5: **Exit the DTS server configuration display**. Type `q` at the prompt and press [RETURN] to exit the DTS server configuration display.

6.4.5.3 Configure Audit Server Option

Follow the steps below to configure the host as an audit server.

STEP 1: **Select the `Configure Audit` server option**. Select the `Configure Audit` server option from the `DCE` option cascading menu.

STEP 2: **Determine if you want to continue with the audit server configuration**. Type `Y` or `N` at the prompt and press [RETURN].

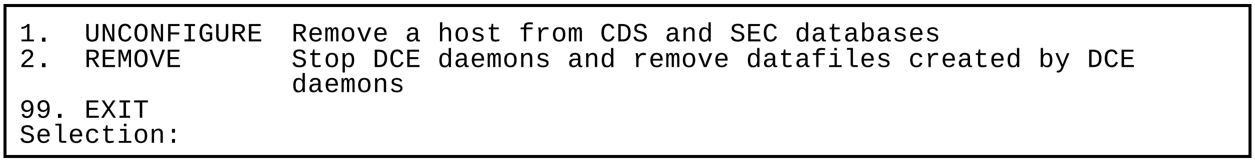
STEP 3: **Exit the audit server configuration display**. Type `q` at the prompt and press [RETURN] to exit the audit server configuration display.

6.4.5.4 Unconfigure DCE Option

The `Unconfigure DCE Client` option allows the system administrator to remove the system as a client from a DCE cell. The interface is through a series of prompted questions and responses from a terminal emulator window.

> **NOTE**: Do not continue with the client configuration if a server is not configured and operating.

Select the `Unconfigure DCE Client` option to open the `DCE Setup` window (Figure 33).



```
1.  UNCONFIGURE  Remove a host from CDS and SEC databases
2.  REMOVE       Stop DCE daemons and remove datafiles created by DCE
                 daemons
99. EXIT
Selection:
```

Figure 33. DCE Setup Window

Follow the steps below to unconfigure the DCE client.

STEP 1: **Choose to unconfigure the DCE client**. Type `1` at the prompt and press [RETURN].

STEP 2: **Enter the cell administrator's account name**. Enter the cell administrator’s account name at the prompt and press [RETURN].

STEP 3: **Enter the password of the cell administrator**. Enter the password at the prompt and press [RETURN].

STEP 4: **Determine if you want to force unconfiguration**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 5: **Exit the DCE client configuration display**. Type `q` at the prompt and press [RETURN] to exit the DCE client configuration display.

6.5 Removing Global Data

The COERemoveGlobal command line tool allows the system administrator to remove global segment data on the global users/profile workstation This should be done only if all segments referring this profile have been deinstalled. The specified segment must be available currently on the local workstation. When removing an Account Group segment, the whole directory will be removed (e.g., h/USERS/global/Profiles/SampleAcctGrp).

Follow the steps below to use the COERemoveGlobal command line tool.

STEP 1: **Log in**. Log in as sysadmin.

STEP 2: **Enter the appropriate password**. Enter a password for the sysadmin user.

STEP 3: **Open a terminal emulator window**.

> **NOTE**: Command line tasks are performed in terminal emulator windows. Follow the steps below to access a terminal emulator window.
>
> STEP 1: Double-click on the Application Manager control on the CDE Front Panel to open the Application Manager window.
>
> STEP 2: Double-click on the DII_APPS folder in the Application Manager window to open the Application Manager - DII_APPS folder.
>
> STEP 3: Double-click on the SA_Default folder to open the Application Manager - SA_Default window. This window contains both a Dtterm icon and an Xterm icon.
>
> STEP 4: Double-click on either the Dtterm icon or the Xterm icon to open the window.

STEP 4: **Log in**. Log in as sysadmin at the terminal emulator prompt.

STEP 5: **Enter the appropriate password**. Enter a password for the sysadmin user.

STEP 6: **Remove global data for the specified segment**. Type the following at the prompt:

```
COERemoveGlobal [flags] segment[RETURN]
```

NOTE: If you need help, type `COERemoveGlobal` without any parameters. The following message appears:

```
Usage: COERemoveGlobal [flags] segment
The usable flags are:
-h, h, ?:   Displays the help message
-V:      Displays the version number of the tool
-p <path>   Use path to reestablish path for subsequent filename
This tool will remove global data for the specified segment.
NOTE: If no Path is specified, /h will be used.
```

STEP 7: **Determine if global data has been deleted for the specified segment**. If the command was successful, the following message appears:

```
Successful Removal of Global Data for Segment [segment name]
```

If the command was not successful, the following message appears:

```
Unsuccessful Removal of Global Data for Segment [segment name]
```

The prompt then reappears.

6.6 CSE-SS Functionality

6.6.1 CSEXDM

6.6.1.1 Overview

The X Display Manager (XDM) segment provides users with the capability to log in to a DII COE workstation via a graphical user interface (GUI). The `/h/COE/Comp/CSEXDM/bin/xdm` executable is a modified version of the X11 Release 4, X Display Manager and is initiated as part of the workstation's boot sequence.

6.6.1.2 CSEXDM Configuration

Resources affecting XDM functionality and various GUI characteristics initially have predefined default values. These resource values can be altered from the default settings by modifying various configuration files. Access with `root` privileges to a terminal emulator window and a text editor is required to perform these modifications.

The following is the main configuration file used by CSEXDM:

```
/h/COE/Comp-/CSEXDM/data/config/xdm-config
```

This file contains XDM resources in the X resource format. These resources control the behavior of CSEXDM.

It should be noted that because CSEXDM can manage more than one display connection (e.g. X-terminals connected to the host machine), some of the resources apply to a single display device (per-display resources), while others apply to the CSEXDM process in general (global resources). For per-display resources, values are assigned using the following syntax, where `#` is the display number:

```
   DisplayManager._#.resource:   value
```

To assign a per-display resource value to all displays, an asterisk is used as a wild card in place of the `_#` (e.g., `DisplayManager*resource: value`). For global resource values, a simple dot notation is used (e.g., `DisplayManager.resource: value`).

Table 1 explains the resources set within the `xdm-config` file and shows their default settings.

Table 1. xdm-config File Resource Settings

Resource	**Default Setting**	**Description**
`terminateServer`	`true`	Specifies if the X server should be terminated when a session terminates instead of resetting it.
`systemPath`	`/usr/bin:/usr/sbin/usr /openwin/bin:/etc (etal.)`	Specifies the default value for the PATH environment variable for root users.
`userPath`	`/usr/bin:/bin:/usr/sbin:/usr /local/bin (etal.)`	Specifies the default value for the PATH environment variable for normal users.
`authorize`	`false`	Controls if CSEXDM generates and uses authorization for the server connections.
`resources`	`/h/COE/Comp/data /app-defaults/xdm-resources`	File defining the CSEXDM authentication widget's resources. These resources control the appearance of the CSEXDM opening login window.
`startup`	`/h/COE/Comp/CSEXDM/data/etc /Xstartup`	File containing commands executed by CSEXDM when the windowing session is started.
`session`	`/h/COE/Comp/CSEXDM/data/etc /Xsession`	File containing commands executed by CSEXDM when the windowing session is initialized.
`reset`	`/h/COE/Comp/CSEXDM/data/etc /Xreset`	File containing commands executed by CSEXDM when the windowing session is terminated.
`serverEnv`	`/h/COE/Comp/CSEXDM/data /config/xdm-env`	File containing extra environment variable assignments required by CSEXDM.
`screensaverTimeout`	`5`	Specifies the number of minutes before an inactive login screen is blanked.
`rootLogins`	`false`	Specifies if logins are allowed by root users (users having an ID of 0).

Table 1. xdm-config File Resource Settings

Resource	Default Setting	Description
`servers`	`/h/COE/Comp/CSEXDM/data/config/xdm-servers`	File that contains an entry for each of the displays that should be managed by CSEXDM.
`errorLogFile`	`/h/COE/Comp/CSEXDM/data/log/xdm-errors`	File where CSEXDM errors are written. This file will also contain any errors generated by the Xstartup, Xsession, and Xreset files.
`consoleLogFile`	`/h/COE/Comp/CSEXDM/data/log/xdm-console`	File where console messages are written.
`pidFile`	`/h/COE/Comp/CSEXDM/data/log/xdm-pid`	File where the process identification of the CSEXDM process is stored.
`dbmFile`	`/h/COE/Comp/CSEXDM/data/etc/xdmlogin`	Directory and base filename for the database file that record the number of log in failures for each user.
`maxInvalidLogins`	`3`	Maximum number of log in failures before the user is locked out of the workstation.
`loginResetTimeout`	`1440`	Number of minutes before a workstation with invalid login attempts is reset to zero log in attempts (24 hours).
`lockoutMailRecipient`	`secman`	Specifies the user or mail alias to receive mail messages when users are locked out of a workstation.
`lockoutMailSubject`	`User Locked Out`	Specifies the subject line for mail messages sent when users are locked out of a workstation.
`dceAuthenticate`	`false`	Specifies if DCE user authentication is performed.
`dceLogin`	`/usr/bin/dce_login`	Specifies the default path for invoking the DCE login script.
`useDisplayConsole`	`true`	Specifies if the Console Window will be displayed when CSEXDM is executed.

NOTE: After resource modification, the workstation must be rebooted to effect the changes made.

6.6.1.3 Environment Variables

Alter the environment variables in the `/h/COE/Comp/CSEXDM/data/config/xdm-env`file as appropriate for the site.

6.6.1.4 CDE Invocation

CSEXDM is preconfigured to invoke the CDE desktop upon a successful login. By default, it determines if CDE has been installed by testing for the existence of /usr/dt/bin/Xsession (see /h/COE/Comp/CSEXDM/data/etc/Xsession). If that file exists, it assumes CDE is properly configured and starts up the CDE Xsession script. If /usr/dt/bin/Xsession is not found, it assumes CDE has not been installed and defaults to invoking the MWM window manager as the user session. In this case the mwm binary should exist in one of the path components specified by the DisplayManager*userPath resource in the xdm-config file.

6.6.1.5 Unlocking a Locked Out User

To unlock users previously locked out due to too many invalid login attempts, invoke the CSEXDM_User_Account_Information binary. This binary opens a window that displays a variety of user login information, such as whether the user is currently logged in, the user's full name, and the user's home directory. Users who have an uppercase L next to their name are locked out users. To unlock a user in this condition, highlight the user name then choose clear_failures from the File menu. Repeat this process for all locked out users who are to be unlocked.

The CSEXDM_User_Account_Information binary also can be used to unlock locked users on remote hosts. To view user information on a remote workstation, an entry in the remote systems /.rhosts must exist for the local system. For example, if CSEXDM_User_Account_Information is being run from workstation A the following entry must exist in workstation B's /.rhosts file:

```
A      root
```

For more information, view the User_Account_Information.1 manual page located in /h/COE/Comp/CSEXDM/man.

On platforms where the CSEXDM_User_Account_Information binary is not available, the CSEXDM_clear_failures binary can be used to unlock locked users. Execute the following command as the root user from the shell prompt in a terminal emulator window, where uname is the user name of the locked out user:

```
CSEXDM_clear_failures uname
```

Refer to the clear_failures.1 manual page for more information.

6.6.1.6 DCE

The segment can be configured to perform DCE user authentication against the local cells Security Registry and to download the user security credentials. To enable this feature, first make sure the system has been properly configured to be a DCE client; this should be tested by invoking /usr/bin/dce_login with a valid user name and password. Second, set the DisplayManager*dceAuthenticate resource to true in the /h/COE/Comp/CSEXDM/data/config/xdm-config file. Finally, reboot the workstation. CSEXDM_xdm then should attempt to perform a DCE authentication in addition to the local UNIX authentication.

If the DCE authentication fails and the user is a valid UNIX user, the user is still permitted access to the system; however, the user will not have any DCE security credentials for his or her login session.

6.6.1.7 Servers

In the file /h/COE/Comp/CSEXDM/data/config/xdm-config if the value of the DisplayManager.servers resource is set to /h/COE/Comp/CSEXDM/data/config/xdm-servers, then modify the xdm-servers file according to the xdm.1 manual page. The xdm.1 manual page is located in /h/COE/Comp/CSEXDM/man.

6.6.1.8 Manual Pages

The xdm.1, User_Account_Information.1, and clear_failures.1 files in the /h/COE/Comp/CSEXDM/man/ subdirectory are the on-line manual pages for the CSEXDM_xdm, CSEXDM_User_Account_Information, and CSEXDM_clear_failures applications.

6.6.2 CSECON

6.6.2.1 Overview

The CSECON segment provides a console window (read-only window) that remains open for the life of the user’s login session and cannot be closed, although it may be iconified.

The console window, /h/COE/Comp/CSECON/bin/CSECON_xdcons, is started by CSEXDM and displays error and notification messages written to standard error and /dev/console during the login session. Errors generated by CSECON_xdcons are stored in the /h/COE/Comp/CSEXDM/data/log/xdcons-errors file. The Close function on the CSECON window is disabled by specifying the following resource in the following /usr/lib/X11/app-defaults/Mwm resource file:

```
   Mwm*xdcons*clientFunctions: -close
```

All xdcons resources are specified in the /h/COE/Comp/CSEXDM/xdcons-resources file and described in the Table 2, CSECON Resources.

Table 2. CSECON Resources

Resource	Default Setting	Description
`foreground`	`old lace`	Defines the color of text displayed in the console window.
`background`	`darkslategrey`	Defines the background color of the console window.
`iconic`	`true`	Defines the initial iconified state of the console window.
`geometry`	`+0+0`	Defines the location of the console window on the screen. These coordinates resolve to the upper left corner of the screen.
`text.columns`	`80 columns`	Defines the number of columns the console will display.
`text.rows`	`4 rows`	Defines the number of rows console window will display.
`minHeight`	`39 pixels`	Defines the minimum height to which the console window can be reduced.
`minWidth`	`36 pixels`	Defines the minimum width to which the console window can be reduced.
`heightInc`	`13 pixels`	Defines the height of the icon used to represent the console window.
`widthInc`	`6 pixels`	Defines the width of the icon used to represent the console window.
`title`	`Console Window`	Defines the title of the console window.
`iconName`	`Console`	Defines the title of the window icon.

6.6.2.2 Turning Off the Console Window

For some of the platforms supported by DII COE, the opening of the console window can be prevented by setting a resource value. If the resource `DisplayManager*useDisplayConsole` exists in the `/h/COE/Comp/CSEXDM/data/config/xdm-config`file, the console window can be disabled. To disable the opening of the console window, set the default value from true to false. To enable the opening of the console window, set the value to true. Superuser privileges and a text editor are required to modify the `xdm-config` file. To make the change effective, the user must log out and log in again. Setting this resource value determines the console window configuration for all users local to that workstation.

6.6.2.3 Manual Pages

The `xdcons.1` file in the `/h/COE/Comp/CSECON/man/`subdirectory is the on-line manual page for the `CSECON_xdcons` application.

6.6.3 CSEPAS

6.6.3.1 Overview

The CSEPAS segment provides users with the capability to change their own passwords and provides the security manager with the capability to assign a password to a general user. Both of these utilities use a rule-based password checking capability.

The user can change his or her own password through invocation of the `CSEPAS_userpass` executable. `CSEPAS_userpass` allows the user to enter a new password and re-enter the password for verification purposes. The `/h/data/app-defaults/CSEPAS`resource file is used for setting the font and color characteristics of the GUI windows. `CSEPAS_userpass` implements the public domain `passwd+` software, which provides its rule-based password checking capability. The `/h/COE/Comp/CSEPAS/data/passwd.data`file contains the construction rules for a valid password. The rules contained in this file are discussed in the next section.

The security manager assigns passwords to users through invocation of the `CSEPAS_Assign_Passwords`executable. `CSEPAS_Assign_Passwords`displays a selectable list of users currently existing on the system. `CSEPAS_userpass` is invoked for each user that is selected for password assignment.

6.6.3.2 Changing Password Construction Parameters

To determine the parameters by which a password is constructed, the appropriate set of rules in `/h/COE/Comp/CSEPAS/data/passwd.data`must be selected. To modify the `passwd.data` file, superuser privileges are required. It is recommended that the rules themselves not be modified, with the exception of the password length rule. The desired combination of rules can be selected through the insertion or removal of commenting marks at the beginning of the rules records. A standard ASCII text editor can be used to modify the `passwd.data` file. When the `passwd.data` file is in its initial state, a default set of password rules are selected.

In the case of every rule, to prevent the use of a rule in the construction of a password, comment out the rule by inserting a `#` character at the beginning of the line where the rule is specified. Be aware that some rules are interrelated and may require all associated rules to be commented out to prevent the checking of that password construct. Uncomment the rule by deleting the `#` from the beginning of the line where the rule is specified.

In the `passwd.data` file, the password rules are found beginning on line 102. The first rule of the set disallows the user’s login name being used as his or her password. Note that to allow users to use their log in name as their password the circular shift rule, identified in a following paragraph, must also be commented out. The second rule is similar to the first rule and disallows the use of the user’s log in name typed in reverse being used as their password.

The third through the eleventh rules, discussed in the following paragraph, depend on the GECOS information having been included in the user's password record. If this information is not included with the password record, then these rules are not checked in the construction of new passwords.

The third and forth rules disallow the user's first name and reversed first name being used as their password. The fifth and sixth rules disallow the user's last name and reversed last name being used as their password. The seventh and eighth rules disallow the user's office and reversed office being used as their password. The ninth and tenth rules disallow the user's phone number and reversed phone number being used as their password. The eleventh rule disallows the user's initials being used as their password.

The twelfth and thirteenth rules disallow the newly entered password from being the same as the previous password. The last rule in this section disallows the use of the user's ID from being the password or being contained within the password.

The next rule found in the `passwd.data` file disallows use of a circular shift of the user name as a password.

The next section of the file contains five rules that govern the use of host name and domain name in the construction of passwords. The first two rules in this section disallow the host name and reversed host name of the local workstation being used as passwords. The next two rules disallow the domain name and reversed domain name being used as passwords. The last rule disallows domained host name being used as a password.

The next section of the file contains four rules that disallow words that are found in two separate dictionary files from being used as passwords. Note that both of the rules for a dictionary must be commented out to allow words found in that dictionary to be used as passwords. The two dictionary files are `/h/COE/Comp/CSEPAS/data/trivial.dict`and `/h/COE/Comp/CSEPAS/-data/full.dict`

The last rule in the file determines the required length of the password. The default length of a constructed password is eight characters. To adjust the length of the constructed password change the value of the number after the < character to the minimum desired length. The password can be adjusted to be 1 to 8 characters long. For the benefit of the user, it is suggested that if the password length limit is modified, that the length specified in the error message portion of the rule also be changed to reflect the new length. If this rule is commented out a password from length 1 to 8 characters can be constructed.

6.6.3.3 Manual Pages

The `userpass.1`, `Assign_Passwords.1`, and `passwdplus.1` files in the `/h/COE/Comp-/CSEPAS/man/` subdirectory are the on-line manual pages for the `CSEPAS_userpass` and `CSEPAS_Assign_Passwords` applications.

6.6.4 CSELCK

6.6.4.1 Overview

The CSELCK (xlock) segment provides the DII COE with an automatic session locking mechanism that activates when the mouse and keyboard have been idle for a configurable amount of time.

6.6.4.2 Operation

The condition of a session when it is in an idle state is referred to as deadman. The CSELCK segment considers deadman to have two distinct phases. During the first phase of the deadman, `/h/COE/Comp/CSELCK/bin/CSELCK_xautolock`automatically locks the screen if the keyboard and mouse have been idle for a configurable time limit by invoking `/h/COE/Comp/CSELCK/bin/xlock` During the second phase of the deadman, xlock takes a deadman action if the keyboard and mouse remain idle for a configurable time limit after the screen has been automatically locked. The xlock resources are specified in the file `CSELCK` located in the `/h/COE/Comp/CSELCK/data/app-defaults`subdirectory. These resources are described in Table 3. Superuser privileges and a text editor, such as “vi” editor, are required to change this file. The xlock resources are located at the end of the `CSELCK` file. At the beginning of this file, after some records of modification, are the settings for the various screen saver modes which are used by the `CSELCK_xlock` screen locking application. The settings for these screen saver modes are described in the `CSELCK_xlock` manual pages.

Be aware that the CDE which comes with the DII COE kernel also contains a screen saver function. Depending on whether it is enabled and the settings of its time out value, it may engage before the CSELCK can perform its session locking function.

6.6.4.3 Changing Screen Lock Time Out

The `CSELCK_xautolock` process is initially invoked when xdm executes “ Xsession” during user log in. This file is located in the `/h/COE/Comp/CSEXDM/data/etc/`subdirectory. This file must be edited to change the period of time that `CSELCK_xautolock` waits before locking the screen of an idle workstation. Superuser privileges and a text editor, such as “vi” editor, are required to change this file. This task is intended to be performed by the System Administrator. The `-time` option of the command line which invokes the `CSELCK_xautolock` process is the value which needs to be changed. The command line appears as follows:

```
if [ -d /h/COE/Comp/CSELCK ]; then
   /h/COE/Comp/CSELCK/bin/CSELCK_xautolock -time 5 -locker
   “/h/COE/Comp/CSELCK/bin/CSELCK_xlock -name CSELCK
   -remote -allowaccess +allowroot >&- 2>&-” &
fi
```

Note that the line is replicated here with the default options. The maximum value that the `-time` option can be is 60 minutes and the minimum value is 1 minute, the default, as shown, is 5 minutes. The workstation must be rebooted after the change is made to make it effective.

Table 3. CSELCK (Xlock) Resources

Resource	Default Setting	Description
deadmanTimeout	30 minutes	Specifies the number of minutes after the screen is locked to execute the deadman action.
deadmanAction	none	Specifies the actions to be performed when deadman timeout expires. It may consist of the string "none" or one or more of the following space separated strings: "notify", "terminate", and "script". If "none" is set, no action will be performed. If "notify" is set, the person or mail alias, specified by the deadmanMailRecipient resource, will be notified by email that the workstation has been left unattended. If "terminate" is set, the user's session, including all processes owned by the user, will be terminated. If "script" is set, the shell script named by the deadmanScript resource will be executed.
deadmanWarningTimeout	60 seconds	Specifies the number of seconds before executing the deadmanAction to display a warning message.
deadmanWarning	Depends on the setting of the deadmanAction resource	Specifies the warning message to display. If the deadmanAction contains the "terminate" flag, the deadmanWarning default is "WARNING: Inactive session will be terminated in %d seconds!". Otherwise the default is to not display a warning message.
deadmanWarningBell	on	Controls whether an audible beep is sounded at one-second intervals during the display of the warning message.
deadmanScript	No default	The script executed when the deadman timeout expires if the deadmanAction resource is set to "script". The script must reside in the `/h/CSELCK/data/etc` directory.
deadmanMailRecipient	secman	Specifies the user or mail alias used by the deadman capability when sending mail messages.
deadmanMailSubject	Deadman Timeout	Specifies the subject line of deadman mail messages.

6.6.4.4 Manual Pages

The `CSELCK_xautolock.1` and `CSELCK_xlock.1` files in the `/h/COE/Comp/CSELCK/man/` subdirectory are the on-line manual pages for the `CSELCK_xautolock` and the `CSELCK_xlock` applications.

7. Security Administration Command Line Utilities

Two security administration tasks may be completed by using the command line: changing the security level of a workstation and auditing. These tasks are described in the following subsections.

7.1 Changing Workstation Security Levels

The `COESecLevel` command line tool can be used by the system administrator to change the security level of a workstation. Follow the steps below to use `COESecLevel`.

STEP 1: **Log in**. Log in as sysadmin.

STEP 2: **Enter the appropriate password**. Enter a password for the sysadmin user.

STEP 3: **Open a terminal emulator window**.

> **NOTE**: Command line tasks are performed in terminal emulator windows. Follow the steps below to access a terminal emulator window.
>
> STEP 1: Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.
>
> STEP 2: Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS`folder.
>
> STEP 3: Double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window. This folder contains both a `Dtterm` icon and an `Xterm` icon.
>
> STEP 4: Double-click on either the `Dtterm` icon or the `Xterm` icon to open the window.

STEP 4: **Log in sysadmin**. Log in as sysadmin at the terminal emulator prompt.

STEP 5: **Enter the appropriate password**. Enter a password for the sysadmin user.

STEP 6: **Change the security level of the workstation**. Type the following at the prompt:

```
COESecLevel [security level][RETURN]
```

> **NOTE**: If you would like a list of the security levels or need help, type `COESecLevel` without any parameters. The following message appears:
>
> ```
> Usage: COESecLevel Security Level> is UNCLASS, CONFIDENTIAL, SECRET, TS,
>        SCI.
> ```
>
> (`TS` stands for top secret; `SCI` stands for sensitive compartmented information.)

STEP 7: **Close the terminal emulator window**. Type the following command at the prompt:

```
logout [RETURN]
```

STEP 8: **Reboot the system**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?`Click on the `OK` button to reboot the machine.

STEP 9: **Log in as sysadmin or secman**. The security banner does not depend on the user.

STEP 10: **Enter the appropriate password**. The security banner will have changed to show the new security level.

7.2 Auditing

7.2.1 Auditing on Solaris

Enabling Auditing

Auditing on Solaris can be started automatically after initial kernel installation by typing `Y` at the following prompt: `This script is used to enable the Basic Security Module (BSM). Shall we continue with the conversion now (y/n)?` Refer to the *DII COE Kernel Installation Guide (Solaris 2.4)* or the *DII COE Kernel Installation Guide (Solaris 2.5.1)* for information on starting auditing automatically after initial kernel installation.

If auditing on Solaris was not started after initial kernel installation or has been disabled, auditing can be enabled by logging in as `root` and executing the shell script `/etc/security/bsmconv`, which configures the Basic Security Module.

NOTE: Auditing can only be enabled or disabled by the root user.

After the `bsmconv` command has been run, the system must be rebooted to initialize the auditing subsystem.

Disabling Auditing

Auditing is disabled by logging in as `root` and executing the shell script `/etc/security/bsmunconv`. The system must be rebooted after this script is executed.

7.2.2 Auditing on HP

Enabling or Disabling Auditing From SAM

NOTE: Refer to vendor documentation for more information on using SAM.

Follow the steps below to start or stop audit from SAM.

STEP 1: **Invoke SAM**.

STEP 2: **Select the `Auditing and Security` option**.

STEP 3: **Select either the `Users`, `Events`, or `System Calls` option**.

STEP 4: **Convert to a trusted system**. The following message appears:

```
          You need to convert to a Trusted System before
          proceeding.
The conversion process does the following things:

6.  It saves a copy of "/etc/passwd" in the file
    "/etc/passwd.old.sav".
2.  It then moves the passwords from "/etc/passwd" into a new
    "hidden" password database (the file
    "/.secure/etc/passwd").
3.  It invalidates all passwords in "/etc/passwd" by replacing
    them with "*".  For more details, refer to the "HP-UX
    System Security" manual.

          Do you wish to convert to a Trusted System now?
```

Click on the `Yes` button.

STEP 5: **Affirm that you want to convert to a trusted system**. The following message appears:

```
WARNING:   The change to a Trusted System is irreversible!
           Are you sure you want to continue?
```

Click on the `Yes` button.

STEP 6: **Finish with the conversion**. The following message appears:

```
Converting to a trusted system ...
Task succeeded.  Press OK to continue.
```

Click on the `OK` button.

STEP 7: **Turn auditing on or off.** Select either the `Turn Auditing Off` or `Turn Auditing On` option from the `Actions` button on the menu to stop or start audit, respectively.

Using Shadow Password Files

To use a shadow password file on HP, type `/etc/tsconvert`. This utility updates the shadow password file and removes all password information from the default password file. Once this program has completed, the machine must be rebooted.

To discontinue use of a shadow password file on HP, type `/etc/tsconvert -r`. This utility restores the default password file with the actual encrypted password information. Once this program has completed, the machine must be rebooted.

8. Error Recovery Guidelines

> **NOTE**: Never power off the system without first executing a shutdown. Doing so could cause irreparable damage. If the system has already been brought down incorrectly, refer to Subsection 8.4, *Repairing File Systems*.

The following topics are covered:

C Recovering from basic errors

C Troubleshooting multiple monitors

C Identifying hardware problems

C Repairing file systems

C Reporting problems.

8.1 Recovering From Basic Errors

Access to all System Administration menus and options is required to perform error recovery procedures.

> **IMPORTANT**! The following procedures are listed according to "risk factor"—that is, from the least to the greatest risk of damaging files or losing data. Always begin corrective action with the procedure that poses the least risk.

If these steps do not correct the problem, contact the number listed in Section 8.5, *Reporting Problems*.

Options are unavailable:

C Access to options may be restricted for the user's account. Check with the security manager.

Window hangs or menu option has been disabled:

C Select the `Close All` option from the `SA System` pull-down menu (on the System Administration menu bar). All windows launched from the menu bar or from the `DII_APPS` folder will close. Windows launched from the CDE front panel will not close.

Reboot the system:

STEP 1: Notify users on remote monitors that their applications will soon terminate.

STEP 2: Select the `Reboot System` option from the `Hardware` menu on the System Administration menu bar.

STEP 3: Restart the system with user login.

Power up/power down the system with pointer and keyboard operational:

C See Chapter 3, *Operating Guidelines*.

Power up/power down the system with pointer frozen:

STEP 1: Turn off the monitor and peripherals.

STEP 2: Turn off the CPU.

STEP 3: Wait approximately 30 seconds.

STEP 4: Turn on the monitor and peripherals.

STEP 5: Turn on the CPU.

STEP 6: Restart the system with the user login.

Reinstall the DII COE:

STEP 1: Use the original installation tapes if a network installation is not possible.

STEP 2: Follow the instructions to reinstall the DII COE.

8.2 Troubleshooting Multiple Monitors and Keyboards

Monitor or keyboard fails to respond:

C A reboot may solve the problem.

C Rebooting the computer in a multiple monitor environment means all monitors will go down. When working with multiple monitors, contact all users before rebooting.

Monitor is black:

C Make sure the monitor cable is connected properly.

C Make sure the monitor is connected to a power supply and is turned on.

C The video switch may have incorrect input or output, or may be turned off.

Monitor is black with small yellow squares (HP only):

- Make sure each monitor is connected to the correct port on the back of the CPU.

Second monitor in a dual-eye configuration is gray:

- Make sure keyboards are connected correctly. This monitor is the second eye of a dual-eye configuration.

Trackball does not respond:

- Reboot the machine. If this does not work, try using a different trackball. If the trackball still does not respond, there may be a wiring problem in the cable.

Keyboard does not respond:

- Make sure the keyboard is connected properly.

- The keyboard may be connected properly but the monitor may not "echo" the typed characters to the screen. Rebooting the machine usually solves this problem.

8.3 Identifying Hardware Problems

When the workstation is turned on, the CPU runs a hardware check. If the hardware check is successful, the following occurs:

- The system boots from the default boot device.

- The system displays configuration information, followed by the login prompt.

- Observe the boot information for system/hardware problems. If the boot fails, a disk problem has occurred. Refer to the hardware manual for more information.

8.4 Repairing File Systems

If the system was brought down unexpectedly (e.g., power failure, turned off without proper shutdown), it is designed to repair the file system when powered up.

- The system should never be powered down while the file system is being repaired. To do so would cause further damage to the file system.

- If power is fluctuating, leave the system off until power is re-established.

8.5 Reporting Problems

To receive immediate assistance with a problem or to report a problem, call the DII COE hotline at (703) 735-8682 between the hours of 9:00 a.m. to 5:00 p.m. Eastern Standard Time. The hotline is located at the Operational Support Facility (OSF) in Sterling, Virginia.

If a problem cannot be corrected by the procedures described in this document, follow these guidelines to report it:

STEP 1: **Make sure the problem can be repeated**.

STEP 2: **Record pertinent information**. Record the problem, the last steps leading to the problem, and the frequency with which the problem occurs.

STEP 3: **Describe attempts to solve the problem**.

Appendix A - Communications

A.1 The DII COE Network

An HP or a SPARC loaded with the DII COE can be configured as a stand-alone machine or networked in a server/client relationship.

A.1.1 Stand-alone Configuration

A stand-alone machine is its own server. It retains data without relying on a networked server. It shares data (1) through messages transmitted over configured comms ports or (2) by floppy diskette or tape.

A.1.2 Network Configuration

The communications processor holds all track and comms data. When installing software, the communications processor should be installed first, followed by its client machines. Client machines depend on the server for data, especially data from the track database. Communications processor functions include:

C Processing incoming and outgoing messages

C Decoding incoming messages

C Correlating track information

C Routing outgoing messages.

If the server goes down, the Track Database Manager (Tdbm) warning window informs the user that the server is down. Although the user can view track information, no track database actions (local or shared) are processed.

A.2 Interface Description

The DII COE supports two interface types: serial and LAN.

A.2.1 Serial Interface: RS-232, RS 422, MIL-188

A serial interface is used for serial communication between systems. If systems are at the same site, connect them directly. If systems are at different sites, connect them through a secure modem, such as a STU III.

A.2.2 LAN Interface: Ethernet and Fiber Optic Cabling

Ethernet and fiber optic cabling are used to enable communications between two or more workstations on a LAN. Each machine is assigned a unique name and IP address on the network, which are used by system files.

A.2.3 Protocols

A.2.3.1 TCP/IP

Transmission Control Protocol (TCP) moves data in a continuous, unstructured byte stream. It provides full-duplex service, acknowledgment of data received, and data flow control.

Internet Protocol (IP) provides network layer services to the TCP/IP protocol suite. IP is responsible for forwarding packets through a network based on IP addresses. IP relies on TCP to guarantee delivery of packets.

A.2.3.2 X.25

X.25 is used for a Wide Area Network (WAN) of computers connected by a Packet Switching Network (PSN), such as the Defense Data Network "DSNET1". (X.25 is generally used by ashore sites only.)

A.3 Physical Connections

A.3.1 Serial

A.3.1.1 Requirements for a Direct Connection

A 2-, 3-, and 7-pin connection is required to connect systems located in the same installation.

A.3.1.2 Requirements for STU III Connection

The STU III must support an RS-232 connection. If it does not, the user must request an RS-449-to-RS-232 adapter from the manufacturer.

An HP workstation requires a DB 9 female-to-DB 25-male cable. Certain models of STU III require voltage on pins 4 and 20, which the HP workstation does not supply. A special adapter must be used.

A.3.2 LAN

A.3.2.1 Requirements for an Ethernet Interface

- Use an AUI interface with a DB 15-pin connector between the workstation and the transceiver.

- The copper LAN interface may have a BNC connection between transceivers.

- The network must be terminated at both ends. Use a terminating 50W resistor on each end.

- If the workstation is a stand-alone configuration, the LAN connections on the workstation must be terminated. Use a 50W resistor on each end.

A.3.2.2 Requirements for a Fiber Optic Connection

- Use an AUI interface with a DB 15-pin connector between the workstation and the transceiver.

- The transceiveres must reside at each computer connected by fiber optics. These boxes have dual-ring capability to ensure continued transmission.

For example, if a transmission is interrupted by a broken fiber optic or connection, it is automatically routed to the second ring.

A.3.3 X.25

Requirements for an X.25 Connection (HP)

- If the system is configured for DDN communications, the Serial A port must be the DDN/X.25 interface device. No other device may be configured to the TTYA port.

- A DB 15 connects the machine to a modem and encryption device with an X.25 interface.
- The X.25 card provides synchronous RS-232 (DTE) error-free transmission over the PSN.

- There may be many interfaces, such as crypto, modem, or leased line, between the computer and the actual PSN.

A.4 Communication and Broadcast Configuration

Modify fields to configure a communications channel. Keep in mind the following general information:

C Standard comms settings should be used. Changing some settings, such as baud rate, parity, or stop bits, may cause data to be garbled. For example, if messages are garbled, it is likely that the transmitting and receiving sites do not have the same values set for the baud rate and related fields.

C XON/XOFF should never be used for baudot data connections. Toggle on the XON/XOFF checkbox to enable the use of software flow control to stop and resume transmission.

C If the RTS/CTS checkbox is toggled on, hardware flow control is enabled.

C Make sure the comms interface configuration matches the flow control settings.

A.4.1 Starting Comms Channels

A comms channel must be turned on before it can be used.

Turn channels on and off one of two ways:

C Highlight the channel and then select START, STOP, or RESTART from the pop-up menu.

C Toggle the AUTOSTART checkbox ON in the COMMS EDIT window. This turns a channel on at system startup.

The STATUS column indicates status of each channel: ON or OFF.

Important:

C A comms channel can only be turned on if the designated device exists. For example, a DTC comms channel is assigned to TTYC2. If a multiplexer is not connected to the TTYC port, this channel cannot be turned on, but it can be reassigned to an existing port.

C A channel must be ON to open its status window.

Highlight the channel and select the WINDOW pop-up option.

A.4.2 Starting Broadcasts

A broadcast must be turned on before it can be used. Broadcasts are turned on and off using the BROADCASTS option from the FOTC/BCST menu. The BROADCASTS window displays a list of available broadcasts.

Turn broadcasts on and off one of two ways:

C Highlight the broadcast; select START from the pop-up menu.

C Toggle the AUTOSTART checkbox ON in the BROADCAST EDIT window. This turns the broadcast on at system startup.

The STATUS column indicates status of each broadcast: ON or OFF.

A.4.3 Message Transmission

Messages are sent manually (using an XMIT option) and automatically (using a broadcast).
To transmit a message, make sure the communications channel is turned on, the channel is configured properly, and the channel can transmit messages.

NOTE: Manual transmissions are not allowed on the DTC channel; only automatic transmissions are allowed via the DTC broadcast.

To broadcast a message, make sure the appropriate comms channels are running, as described in the previous section, and the appropriate broadcast programs are running, as described below.

A.4.4 Message and Broadcast Headers

To set a default message header for manual transmissions, click DEFAULT in the HEADER EDIT window pop-up menu. This header is used for all options that have a manual transmit capability, such as tracks and overlays.

Each broadcast has its own header. If DEFAULT is selected while creating a header for a broadcast, the broadcast header becomes the default message header. This header is used for manual transmissions and for the broadcast.

A.5 STU III CONFIGURATION

A serial interface comms channel must first be configured for the STU III connection (see Section A.3, *Physical Connections*). Set the device to the port connected to the STU III. Use serial interface defaults for the other settings: `data type=ASCII`, `parity=NONE`, `stop bit=1`, `baud rate=2400`, `data size=8`, `RECV` and `XMIT=ON`.

C An entry must be made in the Auto-Forward Table. (See *Auto-Forward Table* in the *Unified Build User's Guide*.)

C An entry must be made in the Sources reference table if in FOTC mode. (See *Source XREF Table* in the *Unified Build User's Guide*.)

C Both STU IIIs must be in Remote Control Mode with Secure Access Control System (SACS) enabled.

C Both STU IIIs must have proper ACLs loaded.

C STU IIIs with SACS support auto-answer auto-secure-no operators are needed. In this mode, Voice/Secure Voice options are unavailable.

SACS grants access to designated STU IIIs, as identified in the ACL on the local STU III.

Three requirements for secure authentication of automatic, incoming calls are (1) ACL header, (2) DAO code, and (3) Keyset ID.

STU IIIs (including STU III SACS) without these codes are excluded, and cannot gain access or connect with STU-IIIs that share DAO codes or keyset IDs.This creates a closed network. Unauthorized calls are disconnected before the line to JMCIS is opened. If two STU IIIs can talk to each other, but cannot transmit data, their internal modes may be different. Check baud rates: synchronous and asynchronous must match.

A.5.1 Downloading ACL

The following tables illustrate the sequence of an ACL download. This sequence has been tested on AT&T devices only.

STEP 1: Insert the Master CIK.

STEP 2: Click on the `MENU` option.

OBSERVE	PRESS
`Main Menu Secure Voice`	`NEXT`
`Main Menu Secure Data`	`NEXT`
`Main Menu Show Config`	`NEXT`
`Main Menu Change Config`	`SELECT`
`Change Config Security Config`	`SELECT`
`Security Config SACS Disable`	`NEXT`
`Security Config SACS Options`	`SELECT`
`SACS Options SACS Control`	`NEXT`
`SACS Options Auto Access Control`	`NEXT`
`SACS Options Far-end ID`	`NEXT`
`SACS Options Access List`	`SELECT`
`ACCESS LIST MENU Load ACL Via DTE`	`SELECT`
`WAITING FOR ACL start DTE transfer`	(begin download)
`RECEIVING ACL please wait`	(wait until finished)
`ACL RECEIVED nnn show new ACL`	`NEXT`
`ACL RECEIVED nnn save new ACL`	`SELECT`
`NEW ACL SAVED previous menu`	`MENU`

A.5.2 Temporarily Disabling SACS ACL

STEP 1: Insert the Master CIK.

STEP 2: Click on the `MENU` option.

OBSERVE	PRESS
`Main Menu Secure Voice`	`NEXT`
`Main Menu Secure Data`	`NEXT`
`Main Menu Show Config`	`NEXT`
`Main Menu Change Config`	`SELECT`
`Change Config Security Config`	`SELECT`
`Security Config SACS Disable`	`SELECT`
`SACS Disable on/off change Disable`	`SELECT`

A.5.3 Autodialing Between Two AT&T STU IIIs

STEP 1: Insert the Master CIK.

STEP 2: Click on the MENU option to turn auto-answer on.

After the ACL is downloaded, but before it is put in Remote Control Mode, auto-answer must be on.

If the display indicates one or more AASD rings, auto-answer is on.

PRESS	**PRESS**
NEXT until "Change Config"	SELECT
NEXT until "Security Config"	SELECT
NEXT until "SAC Options"	SELECT
NEXT until "SACS Control" (ensure SASCTRL is enabled.)	SELECT

PRESS	**PRESS**
MENU	MENU (again)
NEXT until "Change Config"	SELECT
NEXT until "Security Config"	SELECT
The display panel will read SACS Disable (ensure SACS Disable is OFF)	SELECT

PRESS	**BUTTON**
MENU	MENU (again)
NEXT until "Change Config"	SELECT
NEXT until "Security Config"	SELECT
NEXT until "SAC Options"	SELECT
NEXT until “Auto Access Ctrl”	(Ensure Auto Access Ctrl is ON)

PRESS	**BUTTON**
MENU	MENU (again)
NEXT until"Change Config"	SELECT
NEXT until "Auto-Answer"	SELECT

A.5.4 Configuring Specific STU-III Models

Motorola SECTEL 1000/2000:

C This device provides the auto-secure feature, but does not allow auto-answer, nor does it support SACS.

C The default data mode is 2400 baud, asynchronous.

C An RS-232 port is included, allowing direct connection to the system.

C A serial communications interface must be used.

RCA STU III:

C The STU III data port is an RS-232 (DB 25) or an RS-449 (DB 37) connection, depending on manufacturer and model.

C RS-232 and RS-449 share the same signal levels but have a different pinout.

C RS-449 ports must be converted to RS-232 to work with the system. These converters are included with the STU III.

Table 4 illustrates the conversion requirements of a STU III RS-449 configuration to an RS-232.

RS-449 (STU-III)	RS-232 (TDP)
1–Shield	1–Shield
4–Send Data (+)	2–TXD
6–Receive Data	3–RXD
7–Request to Send	4–RTS
9–Clear to Send	5–CTS
11–Data Mode	6–DSR
19–Common Return	7–Common
20–Receive Common	
22–Send Data (-)	
37–Send Common	
12–Terminal Ready	20–DTR

Table 4. RS-449 to RS-232 Conversion

Follow the steps below to configure an RCA STU III:

STEP 1: Press `PROGRAM`.

STEP 2: Press `SETUP`.

STEP 3: Press `YES` at "`set terminal options`."

STEP 4: Press `YES` at "`set standard options`." The standard settings are:

- Dialing mode: TONE
- Comm mode: FULL DUPLEX
- Data Ports: 2400 ASYNC
- Remote Capable: DISABLED
- A-lead Control: ENABLED
- Dual Home: Line 1 only.

Appendix B - Multiple Monitor and Keyboard Configurations

A single, properly equipped HP TAC-3 (Tactical Advanced Computer) CPU can drive any of the following configurations:

C Single-eye console with 1-3 single-eye remote monitors

C Dual-eye console with 1-2 single-eye remote monitors

C Dual-eye console with a dual-eye remote monitor.

Tables 5 and 6 illustrate the recommended single-eye and dual-eye monitor connection schemes. For potential difficulties the user may encounter in a multi-monitor environment, see Subsection 8.2, *Troubleshooting Multiple Monitors and Keyboards*.

Single-eye Console	**Remote 1**	**Remote 2**	**Remote 3**
Monitor: crt00 Keyboard: KYBD4	None	None	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	None	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	**Single-eye** Monitor: crt10 Keyboard: KYBD3	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	**Single-eye** Monitor: crt10 Keyboard: KYBD3	**Single-eye** Monitor: crt11 Keyboard: KYBD4

Table 5. Single-eye Console

Dual-eye Console	Remote 1	Remote 2
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	None	None
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt10 Keyboard: KYBD4	None
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt10 Keyboard: KYBD3	**Single-eye** Monitor: crt11 Keyboard: KYBD4
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Dual-eye** Top Monitor: crt11 Bottom Monitor: crt10 Keyboard: KYBD3	None

Table 6. Dual-eye Console

Appendix C - Database Size Limits

This appendix lists database limits for various DII COE files.

Tracks	Limits
Platform/Ambiguity	1500
Emitter	1500
Link	1024
Acoustic	100
Unit	500
SI	450
External	0

Table 7. Track Limits

Other Track Ranges	Limits
Confidence Level of AOU Cross-fix Ellipse	90 percent
Dynamic Status Board	1 master track / 20 slave tracks
Land Sites	100
Missile Systems/Track	10
Radar Systems/Track	10
Sonar Systems/Track	10
Weapon Systems/Track	10
Specific IFF Mode-2 Valued Tracks Can Be Archived	20
Track Archive Sequence of Steps	60 seconds
Track Groups	32
Tracks/Group	Limited only by disk storage
Track History Reports/Track	1,000
Track Symbol Label	26 characters

Table 8. Other Track Range Limits

Communications	Limits
Addressee (Channel Message Buffer Manager)	1,000 backlog messages
Alert Log	1,000 messages
Incoming Message Log	1,000 messages
Incoming Opnote Log	200 opnotes
Outgoing Message Log	1,000 messages
RAINFORM Messages	1,000 lines
Received Messages Displayed in Status Window	1,000 messages
Report Log	2,000 reports
Saved for Raw Messages	500 lines

Table 9. Communications Limits

Miscellaneous	Limits
Auto-Forwarding, Addresses	500
Broadcast, User-Set Cycle Rate	0-720 minutes
Broadcasts, Active	25
Characters Stored per Screen Name	50
Clipboard, Files Stored on	1,000
Engagement Scenarios	10
Grid Cells, Number of	24 or 48
IFF/DIs, Nicknames	100
Incoming Message Alert, Addresses	5
Incoming Message Alert, Originators	5
Net Address (DDN)	256
Satellite Charlie Elements	300
Satvul-Satellites per Category	300
Stored Screen, Briefing Slides	50
Stored Screens, Number of	50

Table 10. Miscellaneous Limits

Maps	Limits
Key Sites	1,000
Stored Map, Parameter Combinations	500
Stored Maps	20
Zoom Width, Greatest	21,600 NM
Zoom Width, Smallest	0.25 NM

Table 11. Map Limits

Overlays	Limits
Overlay, Items	100
Overlay, Points	256
Overlay, Polyline Points	256
Overlays, Number of	500

Table 12. Overlay Limits

This page intentionally left blank.